SIEMENS

ARCADIS

SP

Configuration

System

SRS / System Management (MNP)

valid for ARCADIS family VB13C

© Siemens AG 2007
The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Print No.: SPR2-310.843.03.01.02
Replaces: n.a.

English
Doc. Gen. Date: 04.07

Document revision level

The document corresponds to the version/revision level effective at the time of system delivery. Revisions to hardcopy documentation are not automatically distributed.

Please contact your local Siemens office to order current revision levels.

Disclaimer

The installation and service of equipment described herein is to be performed by qualified personnel who are employed by Siemens or one of its affiliates or who are otherwise authorized by Siemens or one of its affiliates to provide such services.

Assemblers and other persons who are not employed by or otherwise directly affiliated with or authorized by Siemens or one of its affiliates are directed to contact one of the local offices of Siemens or one of its affiliates before attempting installation or service procedures.

Table of Contents 3

1 General Information 5

Document description . . . 5
General and product-specific safety hints . . . 5
Screenshots & graphics . . . 5
Abbreviations, definitions . . . 5
Use of document for ARCADIS VB13C . . . 7

2 Prerequisites 8

SRS server concept . . . 8
The SRS server concept . . . 8
SRS access server . . . 9
System management servers . . . 9
SRS portal access . . . 10
SRS routing concept . . . 11
SRS router information . . . 11
SRS router in a network . . . 13
Basic network situations . . . 13
General SRS configuration . . . 14
SRS configuration with outside NAT (Network Address Translation) . . . 17
Configuration of VPN . . . 19
General information . . . 19
Configuration . . . 19

3 Configuration of SRS functionalities 20

SRS configuration process . . . 20
Collection of informations (network-related and others) . . . 21
SRS Router configuration . . . 22
Entering the system into the SRS database . . . 23
Configuration of network settings based on syngo . . . 24
Configuration of network settings for the modality . . . 24
Description of configuration for TCP / IP LAN settings . . . 24
Running the SRS Pre-connect Tool . . . 31
Enable remote access based on syngo . . . 32
Enter the country code and the customer ID . . . 34
Configure FTP transfer based on syngo . . . 35
Configuration of the SRS target (host) used for FTP service . . . 35
Definition of the FTP target . . . 35
Create a test file to check FTP transfer . . . 36
Check FTP transfer . . . 37
Configure access to the knowledge base based on syngo . . . 39
Configure the access to Knowledge base . . . 39
Internet Explorer settings . . . 39

4 Configuration of System Management (MNP) 44

General prerequisites 44
Activating system management 46
1. Activate the option “System Management” 46
2.1. Configuration of SM without NAT 47
2.2. Configuration of SM with Inside NAT 49
2.3. Configuration of SM with Outside NAT 51
3 . Start of activation procedure. 53
4. Check the functionality of all MNP components 55
Deactivating System Management 57
Procedure for deactivating System Management 57

5 Troubleshooting 60

6 Additional information 61

Additional information 61
SRS portal access 61
SRS Help Desk 61
SRS Checklist 61
SRS Toolkit 62
SRS Pre-connect Tool 62
Passwords 62
Country codes 62

7 Changes to previous version 66

Document description

This document describes where information can be obtained and where an active configuration has to be performed for Siemens Remote Service on syngo-based and on Fluorospot Compact systems.

General and product-specific safety hints

Follow the guidelines of general and product-specific safety information when performing maintenance and service work.

Screenshots & graphics

Screenshots and graphics within this document are only examples.

Not all configurable combinations and variants are described in this document.

This document describes the principle and the most common configuration.

Abbreviations, definitions

Abbreviation	Description
BU	Business Unit
CA	Computer Associates
CSE	Customer Service Engineer
CS SD GUI	Customer Services Software Delivery Graphic User Interface
CS ML	Customer Services Material Logistics
EPS	Enhanced Productivity Services e.g. Virus Protection
FTP	File Transfer Protocol
HP	Hewlett Packard
ISDN	Integrated Services Digital Network
LAN	Local Area Network
MNP	Managed Node Package a versioned collection of System Management software and support files for a Medical Solutions system
NAT	Network Address Translation

Abbreviation	Description
RUH	Remote Update Handling (also called Remote Software Update)
SRS	Siemens Remote Service
VPN	Virtual Private Network

Use of document for ARCADIS VB13C

NOTE

The following functions are not released for VB13C:

- System Management

- Remote Software Update (Remote Update Handling = RUH)

- Enhanced Productivity Services (Virus Protection).

SRS server concept

The SRS server concept

The SRS server concept is divided into two parts:

- SRS access server
- System management servers

The **SRS access servers** provide the following functionalities:

- Reactive Remote Service: Remote access to system from headquarters and file transfer from and to the SRS server via FTP protocol.
- Proactive Remote Service (Autoreporting): If the customer's IT environment supports dial out functionality, automatic file transfer from and to the SRS server is possible .

  The automatic file transfer uses the FTP protocol.

The **System management servers** provide the following functionalities:

- Proactive Event Management: Sends a message to the Service Support Center if predefined events occur.
- Remote Software Update: Allows for remote transfer and installation of software updates. The remote update is triggered by headquarters or by the local user.

NOTE	**For Arcadis VB13C, these functionalities are not released.**

The following components of **Enhanced Productivity Services (EPS)** can also be enabled additionally, to enhance the activated system management functionality of the system.

- Utilization Management:

  The system generates workflow-related data and sends them to headquarters for analysis. Based on these data, benchmarking with other customers is possible.

- Virus Protection:

  A Trend Micro scan engine is activated and checks the file system for known viruses. The newest virus pattern is downloaded shortly after its release using System Management - Remote Software Update.

NOTE	**For Arcadis VB13C, EPS (e.g. Virus Protection) is not released.**

NOTE	**Components of EPS may only be enabled as requested by the local service organization because these services are purchased by the customer.**

NOTE

EPS is released only for systems that connect via VPN connections.

SRS access server

Three worldwide access servers (RDIAG) make your system accessible to Siemens Remote Service.

Time zone / server function	**I (Europe, Africa) Fuerth**	**II (America) Newark**	**III (Asia, Australia) Singapore**
SRS Access Server[1] [2] **see note**	LUX09505 **194.138.39.18**	SRSACC1 **129.73.116.92**	SGPT806X **194.138.243.178**

1. This is the target server for the configuration of the FTP transfer functionality in the modality service configuration
2. These servers are connected with a webmask SRS portal, where the CSEs can reactively connect to the modality

NOTE

When the customer uses network configuration with Outside NAT, the IP address will be replaced by the IP address given by the hospital network administrator.

System management servers

Time zone / server function	**I (Europe, Africa) Fuerth**	**II (America) Newark**	**III (Asia, Australia) Singapore**
CA event management **see note**	FTHW9MTA **194.138.39.20**	SRSSQL01 **129.73.116.90**	SGPT3180A **194.138.243.180**
CA asset management **see note**	FTHW9MUA **194.138.39.21**	SRSSQL02 **129.73.116.93**	SGPT3181A **194.138.243.181**
CA software distribution (**MNP access server** [1]) **see note**	FTHW9MVA **194.138.39.22**	SRSSQL03 **129.73.116.94**	SGPT3182A **194.138.243.182**

1. This is the target server for the installation of the Managed Node Package (MNP)

NOTE

When the customer uses network configuration with Outside NAT, the IP addresses of the CA servers will be replaced by the IP addresses given by the hospital network administrator.

SRS portal access

A personal account is required on the SRS portal to access data and connect to systems.

For accounts, see “Contact MMD Country Admin”:

http://cs.med.siemens.de/cms/en/tools/mmdcountryadmin/default.asp

SRS routing concept

SRS router information

SP products are only designed for a router or VPN (Virtual Private Network) connection.

Router connection

The phone line must be a direct ISDN line (not a switchboard). The phone extension should allow international dial-in and dial-out calls to support the new SRS server concept.

NOTE

For using the functionality Enhanced Productivity Services (e.g. Virus Protection) a broadband connection of:

>= 768 Kbit/s Downstream (SRS Servers -> Modality) and

>= 128 Kbit/s Upstream (Modality -> SRS Servers)

is needed.

NOTE

In many countries, the SP system currently has to dial out internationally to contact the server, e.g., for auto-reporting or system management reporting.

For this reason, toll-free numbers for accessing the servers have been established.

VPN

SRS over a VPN connection (Internet) requires:

- a **static** IP address for the **customer's** end point (router equipment)
- a **static or dynamic** IP address for the **Siemens** end point (router equipment)

Network

To connect the router/VPN to the system within the customer LAN, the following IP addresses are necessary:

- one for each modality
- one single address for the SOA equipment (in SOA case --> Siemens router equipment)

Router hardware

A current router hardware list and order form are available in the intranet under SRS Connectivity Toolkit

SRS Toolkit --> see Additional information.

Router administration

The router is administered either by the customer (COA) or Siemens (SOA).

1. **C**ustomer-**o**wned **a**ccess (**COA**)

   The router has to be compatible with the Cisco router used in the SRS server environment.

   Fill out the SRS checklist with the customer-specific data. The SRS help desk will contact the customer and arrange a router configuration. After completion, a confirmation mail is forwarded to the person noted on the SRS checklist.

   SRS Checklist --> see Additional Information.

2. **S**iemens-**o**wned **a**ccess (**SOA**) for **dial up** connection

   Cisco routers are used exclusively. For model type, see the SRS Toolkit under "Additional Information".

   Currently, router configuration is performed by the SRS help desk.

   All routers delivered from the spare parts delivery department (CS ML) are pre-configured. This means that once hardware installation is completed, the SRS Help Desk (CHS IN) can access the router remotely and perform the final configuration.

   To have the final configuration performed, fill out the SRS checklist with the customer-specific data and send it to the address on the checklist. After completion, a confirmation mail is forwarded to the person noted on the SRS checklist.

   SRS Checklist --> see Additional Information

3. **S**iemens-**o**wned **a**ccess (**SOA**) for **VPN** connection

   Cisco routers are used exclusively. For model type, see the SRS Toolkit under "Additional Information".

   Currently, router configuration is performed by the SRS help desk.

   All routers delivered from the spare parts delivery department (CS ML) are pre-configured.

   In this case, the router requires a second preconfiguration step when running a Siemens-specific setup software (broadband configuration wizard).

   The second preconfiguration is performed on a laptop of the CSE or the installation team in cooperation with the SRS help desk.

   The SRS help desk (CHS IN) can access the router remotely and perform the final configuration.

   To have the final configuration performed, fill out the SRS checklist with the customer-specific data and send it to the address on the checklist. After completion, a confirmation mail is forwarded to the person noted on the SRS checklist.

   SRS Checklist --> see Additional Information

SRS router in a network

Basic network situations

Guidelines for configuring SRS router access in the modality.

There are two possible router locations at the customer site:

1. The system and the hospital SRS router are in the same subnet area.

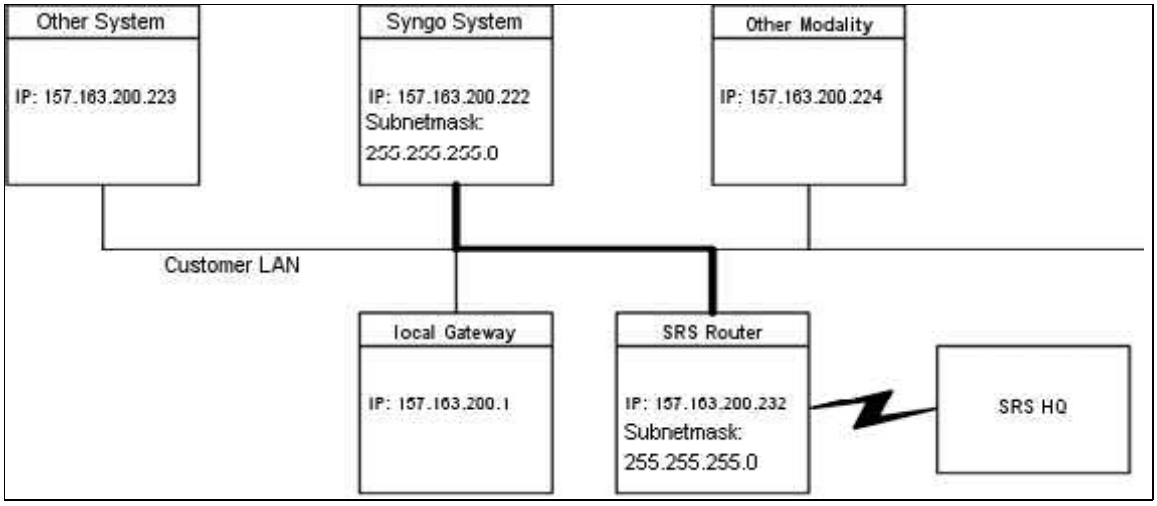

Fig. 1: Modality and hospital SRS router in the same subnet

2. The system is on a different subnet area than the hospital SRS router.

   The hospital network administrator configures the “Gateway to SRS” (example 192.168.170.1 to access the SRS access server in Fürth (Germany)).

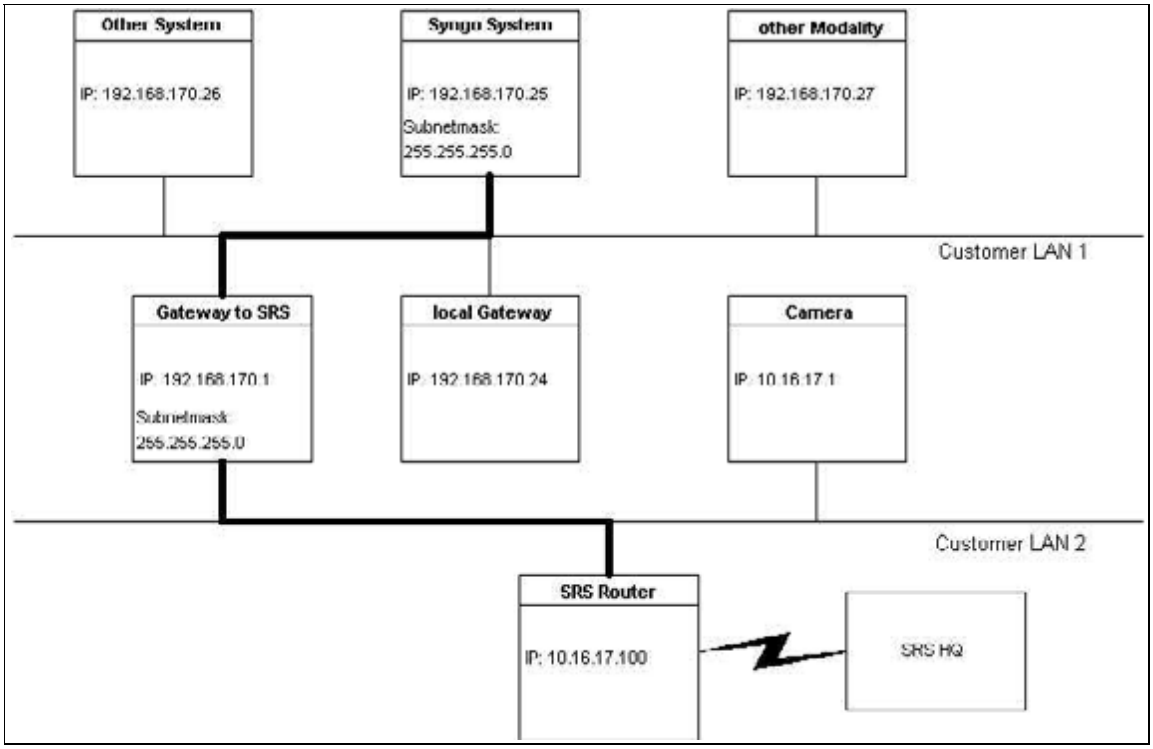

Fig. 2: Modality and hospital SRS router not in the same subnet

General SRS configuration

This chapter describes items common to all of the connected systems, such as SRS configuration.

The modality and the hospital SRS router are in the same subnet

The hospital network administrator need not be involved in the configuration process.

NOTE

The default gateway functionality under Windows XP (TCP/IP gateways) works only for a single gateway IP address.

This means that only one IP address should be entered under TCP/IP gateways.

Normally, the default gateway is already occupied by the customer’s network environment -->

--> the routing from the syngo system to the SRS router is established via a static route.

Setting of static route based on command interpreter for ARCADIS VB13C

For ARCADIS VB13C with syngo VD30A, the configuration via command interpreter is required.

NOTE

Warning:

The static route is not saved by the configuration backup.

The static route has to be entered again after software installation.

Enter a static route by using a command to the operating system.

- Open a command interpreter such as "Escape to OS".
- Enter the static route to the corresponding SRS server as displayed below (SRS server Fürth/Newark/Singapore) in the parameter line.

Command	IP and netmask of SRS server									SRS router IP address				permanent
route add	194.	138.	39.	0	mask	255.	255.	255.	0	157.	163.	200 .	232	-p

SRS server Fürth:	route add 194.138.39.0 mask 255.255.255.0 157.163.200.232 -p
SRS server Newark:	route add 129.73.116.0 mask 255.255.255.0 157.163.200.232 -p
SRS server Singapore:	route add 194.138.243.0 mask 255.255.255.0 157.163.200.232 -p

Explanation:

The syngo system 157.163.200.222 uses the static route to the hospital SRS router 157.163.200.232 to reach the SRS access server 194.138.39.0 (Fürth, Timezone I) without using the local gateway. The -p stands for permanent route.

NOTE

Alternative: Configure the hospital SRS router as the default gateway under TCP/IP LAN gateways if the customer is not using a default gateway.

- In order to save the data, write down the line showing the route to the SRS target server
- Perform a connectivity test as described in the "Troubleshooting" section of this document.

Setting of static route based on syngo internal function

NOTE	**This chapter will not be used for ARCADIS VB13C.**

With higher versions of syngo systems (>= VE30), a separate configuration page is available. As an example, see the following illustration:

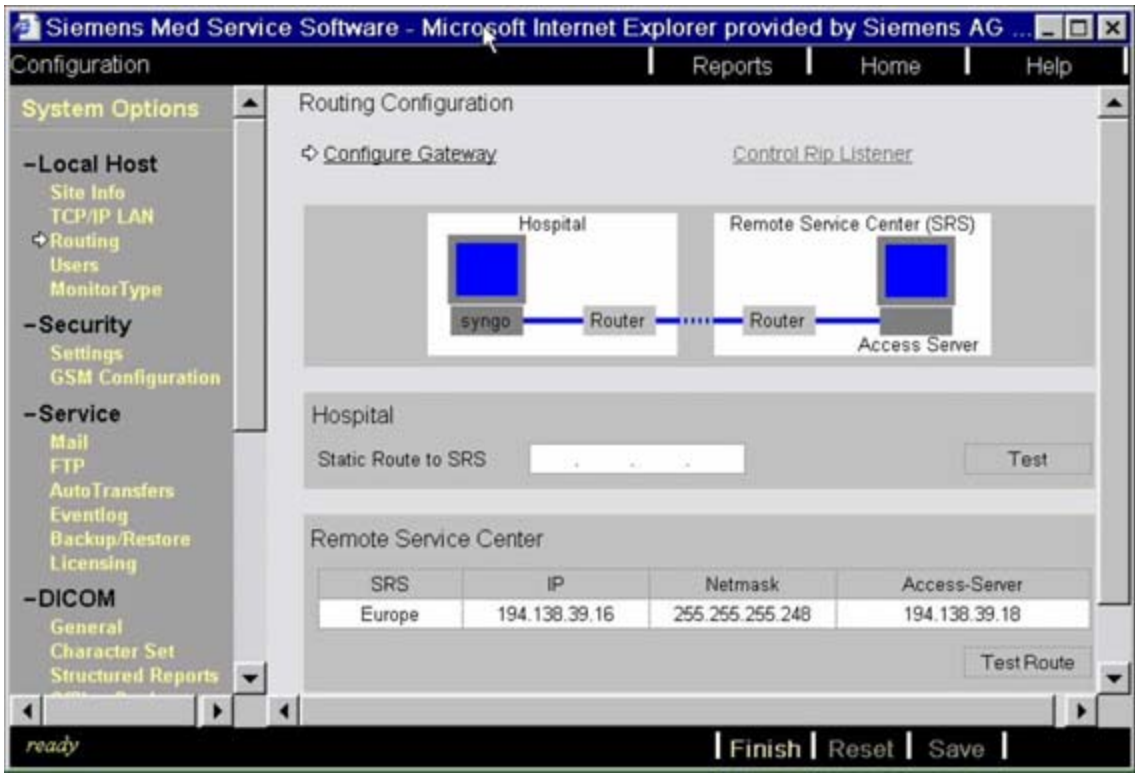

Fig. 3: Routing configuration

NOTE	**Alternative: Configure the hospital SRS router as the default gateway under TCP/IP LAN gateways if the customer is not using a default gateway.**

The modality and hospital SRS router are not in the same subnet

The hospital network administrator has to configure the default gateway for connectivity to the SRS access server. This is done in cooperation with the SRS help desk (CHS IN, Customer Health Service Imaging Network)

NOTE	**Only one gateway entry can be defined. Therefore, this procedure applies to customers with only one default gateway used with the syngo system.**

- Enter the default gateway IP address for the local TCP/IP LAN parameter via Configuration/TCP/IP LAN.
- Reboot system

- Perform a connectivity test as described in the "Troubleshooting" section of this document and

  verify if the route configuration has become permanent.

SRS configuration with outside NAT (Network Address Translation)

Description

Outside NAT means the customer defines certain IP addresses that are used by the SP system to communicate with the Siemens environment (e.g. the SRS access server). If the customer uses this function, the Outside NAT addresses have to be configured in the SRS basic settings; otherwise, SRS will not work.

The customer provides an Outside NAT address for the following SRS servers.

- SRS Access Server (for Fürth, Newark, or Singapore)
- CA Asset Management Server (for Fürth, Newark, or Singapore)
- CA Event Management Server (for Fürth, Newark, or Singapore)
- CA Software Distribution Server (for Fürth, Newark, or Singapore)

How to determine whether there is an outside NAT

There is no check available. Outside NAT requires major changes to the SRS configuration that start in the router configuration.

NOTE	**Therefore, this information should be communicated to the SRS help desk and the CSE by the Siemens project manager prior to the SRS configuration.**

NOTE	**If there are any doubts about Inside / Outside NAT for the system, please ask the SRS help desk**

Adding Outside NAT information to SRS settings

The Outside NAT addresses have to be entered as described below.

- Select **Local_Service --> Configuration --> SRS**

- Enable checkbox **Outside NAT**

  Enter the Outside NAT addresses as described below

SRS Access Server IP	Enter the Outside NAT address of the SRS access server. This address is replaced by the NAT address given by the network administrator.
CA Unicenter Event Server IP	Enter the Outside NAT address of the CA Unicenter Event Management Server. This address is replaced by the NAT address given by the network administrator.
CA Unicenter Asset Server IP	Enter the Outside NAT address of the CA Unicenter Asset Server. This address is replaced by the Outside NAT address given by the network administrator.
CA Unicenter Distribution Server IP	Enter the Outside NAT address of the CA Unicenter Software Distribution Server. This address is replaced by the Outside NAT address given by the network administrator.

- Press <save> to configure SRS with the above Outside NAT addresses.

In case of any questions or problems please contact the SRS help desk, see Additional Information.

Configuration of VPN

General information

VPN stands for virtual private network. A “tunnel” is built up via the Internet between the SRS server and the customer system. The beginning and end of this tunnel are defined by so-called Internet security end points (security end points = IP addresses).

The SRS configuration for VPN is identical to the SRS configuration. Under VPN the default gateway points to the Internet security end points instead of the SRS router, as it is the case of a router connection.

NOTE

COA case: Customer router hardware

SRS over a VPN connection (Internet) requires a static IP address for the customer’s end point.

NOTE

SOA case: Siemens router hardware

SRS over a VPN connection (Internet) works with both kinds of IP address (static or dynamic) for the Siemens end point.

Configuration

The configuration of VPN is performed by:

- hospital network administrator
- Siemens company responsible (e.g., SRS team from CHS IN (Customer Health Service Imaging Network)

The basis for the entry is the SRS checklist. The SRS checklist is available on the intranet,

--> see SRS Checklist in Additional Information.

The network administrator defines the hospital routing and provides the default gateway used by the syngo or FLC system to reach the Internet security end point.

This gateway has to be entered as:

- default gateway, or
- as a static route, if a default gateway is already in use by the syngo or FLC system.

The Siemens company responsible enters the configuration parameters for the SRS server and checks the connection.

SRS configuration process

For the configuration process of SRS following activities are necessary:

No	Actions	Who
1	Collection of informations (network-related and others)	SRS Help desk, PM and Customer admin.
2	SRS router configuration	SRS Help desk, PM and Customer admin
3	Entering the system in to the SRS database	SRS Help desk
4	Configuration of network settings of the modality	Installation team, local IT administration
5	Running of the SRS Pre-connect Tool	Installation team, local IT administration, CSE
6	Enable remote access of the modality	CSE
7	Entering the country code and customer ID	CSE
8	Configuration and check of the FTP tranfer	CSE
9	Configuration and check of the access to the Knowledge base	CSE

Collection of informations (network-related and others)

The Siemens Project Manager (PM) ask the customer for following information:

- all information required to complete the SRS Checklist.
- if Inside NAT or Outside NAT is used in the customer's network.

The basis for the entries is the SRS checklist on the Intranet, see Additional Information.

Person responsible	Actions	Comment
Project Manager (PM)	Performance Collecting of Information	The PM asks the customer admin. for information and sends the SRS Checklist to the SRS help desk (Fax) or email (srs_final.med@siemens.com). The PM asks the customer admin. whether Inside NAT or Outside NAT will be used. The PM delivers the information to the CSE.
Customer admin	Performance Delivery of information	The Customer admin. delivers the information to the PM.
SRS Help Desk	Information	The SRS help desk receives the SRS Checklist.
CSE	Information	The CSE receives all the information from the PM.

For questions, see SRS Help Desk in Additional Information.

SRS Router configuration

The router is configured by:

- the Siemens SRS Help Desk (CHS IN), if a Siemens router exists
- the customer admin in cooperation with the Siemens SRS Help Desk (CHS IN), if a customer router exists.

The basis for configuration is the completed SRS checklist, delivered by the PM.

Person responsible	Actions	Comment
SRS Help Desk	Performance (router configuration)	If Siemens router exists.
Customer admin	Performance (router configuration)	If Customer router exists.
Project Manager (PM)	Information	The PM receives the status when the configuration is completed.

Entering the system into the SRS database

The system is entered into the SRS database during router configuration by the SRS help desk (CHS IN Customer Health Service Imaging Network) or the responsible person in the country.

Person responsible	Actions	Comment
SRS Help Desk	Performance Information	The SRS help desk enters the information on the system in the SRS database. The SRS help desk tests the connection to the system.
Project Manager (PM)	Information	The PM is responsible for switching on the system to test the connection with the SRS servers. The PM is informed when the SRS help desk has entered the system into the SRS database

For questions, refer to section SRS Help Desk in Additional Information.

Configuration of network settings based on syngo

Configuration of network settings for the modality

The following components have to be configured for the system:

- Configuration of computer name -> system hostname
- Configuration of TCP / IP LAN settings
- Configuration of a static route in Windows (if necessary)
- Configuration of Inside NAT or Outside NAT, if used by the customer

Description of configuration for TCP / IP LAN settings

Detect the network situation

To configure the network properly, it is important to find out the actual network situation at customer's site.

Normally, one of two network types may exist at the customer site.

First, find out which is the actual network situation at the customer's site; see (Basic network situations / p. 13).

The modality and the hospital SRS router are in the same subnet

The hospital network administrator need not be involved in the configuration process.

NOTE

The default gateway functionality under Windows XP (TCP/IP gateways) works only for a single gateway IP address.

This means that only one IP address should be entered under TCP/IP gateways.

Normally, the default gateway is already occupied by the customer's network environment.

The routing from the syngo system to the SRS router will be set with a static route.

NOTE

Warning: The static route is not saved by the configuration backup.

The static route has to be entered again after software installation.

1. Configuration of “TCP/IP LAN”

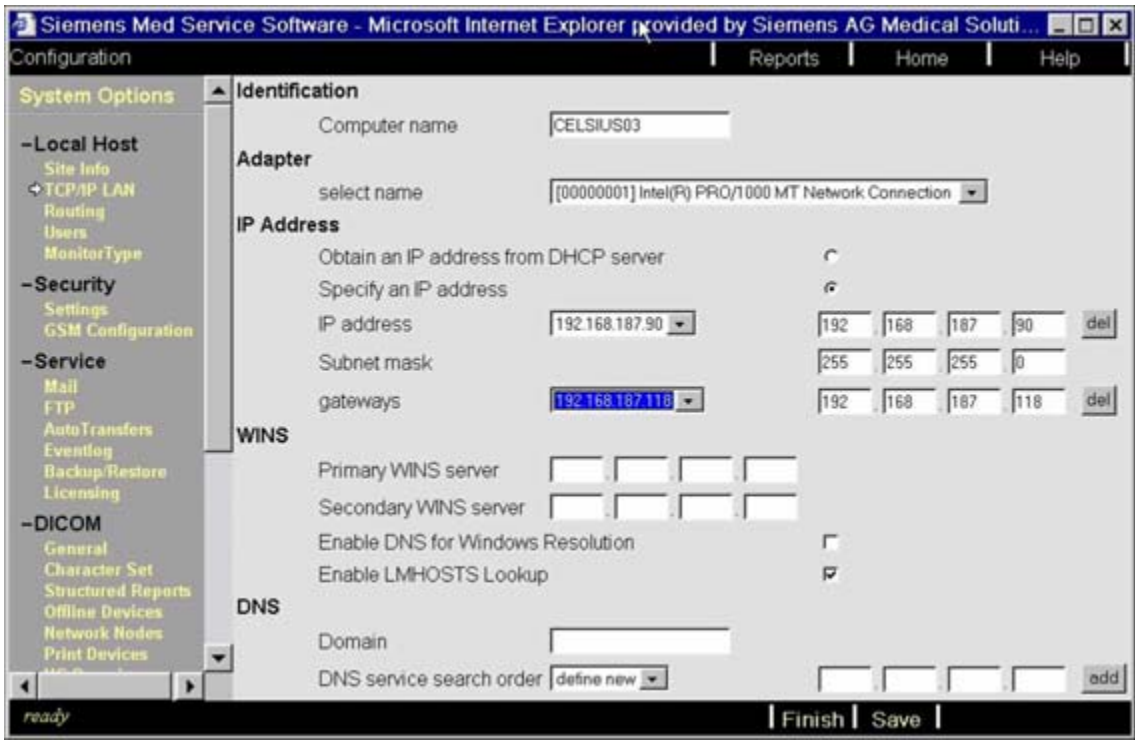

Fig. 4: TCP/IP configuration

NOTE	**Type the IP address of the customer gateway into the “gateways” field.**

Click “Save”

2. Configuration of “Routing” **for ARCADIS VB13C**

   For ARCADIS VB13C with syngo VD30A, the configuration via command interpreter is required.

NOTE	**Warning:** **The static route is not saved by the configuration backup.** **The static route has to be entered again after software installation.**

   Enter a static route by using a command to the operating system.

   - Open a command interpreter such as "Escape to OS".
   - Enter the static route to the corresponding SRS server as displayed below (SRS server Fürth/Newark/Singapore) in the parameter line.

Com-mand	IP and netmask of SRS server									SRS router IP address				perma-nent
route add	194.	138.	39.	0	mask	255.	255.	255.	0	157.	163.	200 .	232	-p
SRS server Fürth:	route add 194.138.39.0 mask 255.255.255.0 157.163.200.232 -p													
SRS server Newark:	route add 129.73.116.0 mask 255.255.255.0 157.163.200.232 -p													
SRS server Singapore:	route add 194.138.243.0 mask 255.255.255.0 157.163.200.232 -p													

Explanation:

The syngo system 157.163.200.222 uses the static route to the hospital SRS router 157.163.200.232 to reach the SRS access server 194.138.39.0 (Fürth, Timezone I) without using the local gateway. The -p stands for permanent route.

NOTE

Alternative: Configure the hospital SRS router as the default gateway under TCP/IP LAN gateways if the customer is not using a default gateway.

- In order to save the data, write down the line showing the route to the SRS target server
- Perform a connectivity test as described in the "Troubleshooting" section of this document.

3. Configuration of “Routing” for ARCADIS > VB13C

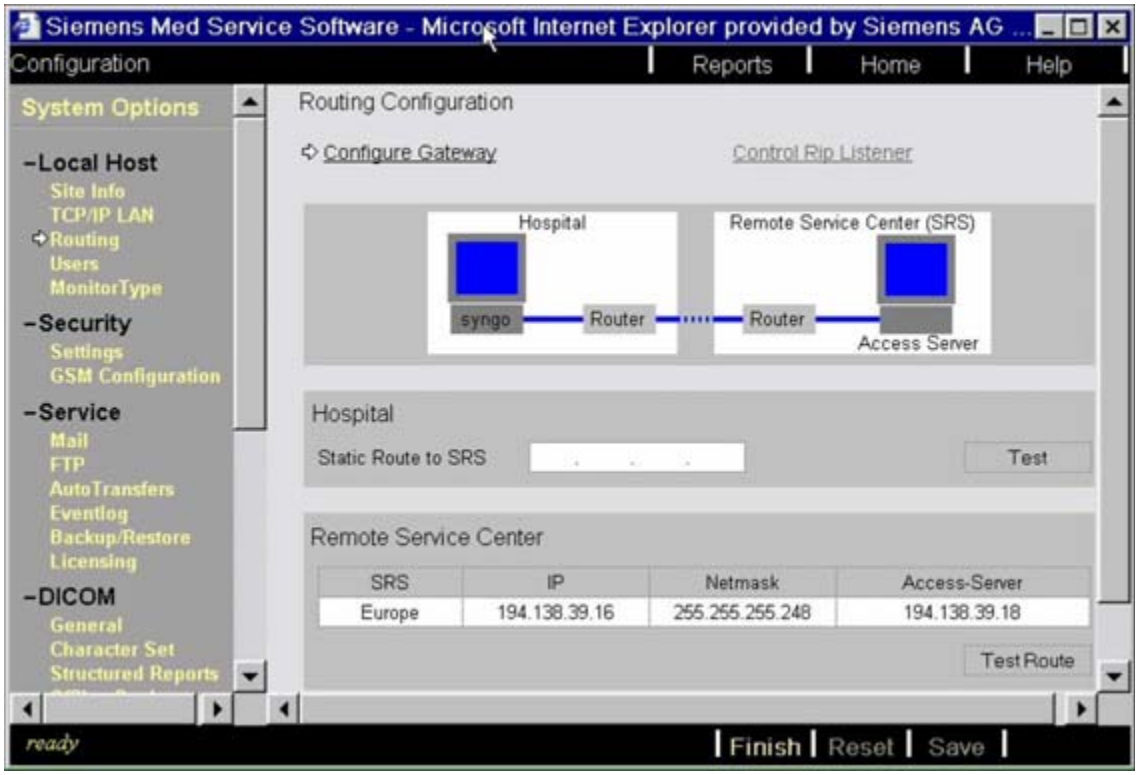

Fig. 5: Routing configuration

NOTE

Type the IP address of the SRS router of the hospital into the field “Static Route to SRS”.

a) Click “Save”
b) Click the “Test” button to check whether the SRS server can be reached over the SRS router of the hospital.
c) Perform the connectivity test described in (Connectivity test / p. 28).
d) If problems occur, call the (SRS Help Desk / p. 61).

The modality and the hospital SRS router are NOT in the same subnet

NOTE

The hospital network administrator has to configure the default gateway for the connection to the SRS access server, see (SRS access server / p. 9).

This is done in cooperation with the (SRS Help Desk / p. 61).

NOTE

Only one gateway entry can be defined. Therefore, this procedure applies to customers with only one default gateway used with the syngo system.

1. Under Local service/Configuration/Local Host, select TCP/IP LAN.
2. Under “gateways”, enter the customer gateway IP address.

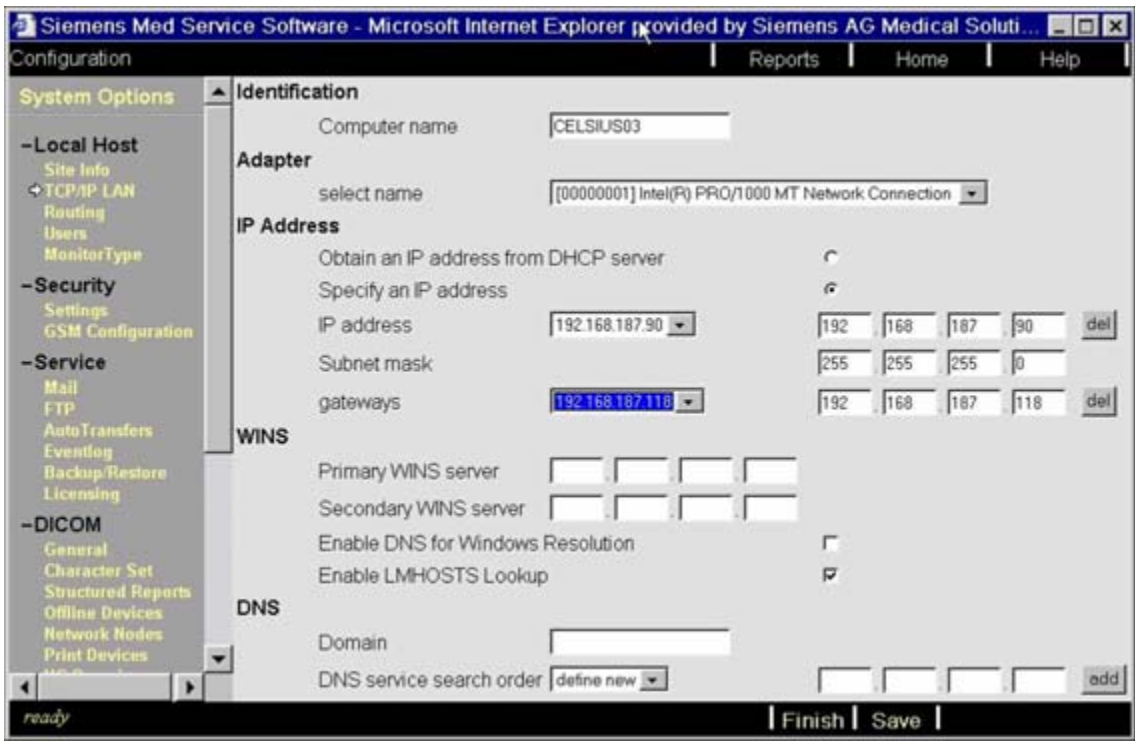

Fig. 6: TCP/IP configuration

3. The configuration of the "routing" page is not necessary in this case.
4. Perform the connectivity test described in (Connectivity test / p. 28).
5. Click “Save” and “Home“ and accept the reboot, if necessary.

Connectivity test

Check the connectivity from the modality to the SRS access server.

Procedure:

- Enable the remote access mode for "Limited Access" or "Limited Access Permanent".
- Select "Utilities" from Service software/Local service/Home menu.
- Select "Escape to OS" in the navigation frame under "Source".
- Select the "NT command interpreter" under "Command".
- Enter the following parameters, depending on the modalities of the access server configuration:

  tracert <ip address of the srs access server of your time zone (SRS access server / p. 9) >

NOTE

The telephone line may need some time to establish the connection. As a result, the tracert program may time out and a message "Destination host is unreachable" or "Request time-out" may appear. Repeat the tracert command and check the connection again.

NOTE

Tracert and ping may not be permitted by the hospital, but the rest of the functionality will work as desired.

e.g. for permitted: country UK, or VPN via COA (customer router)

Example for time zone I, SRS server Fürth

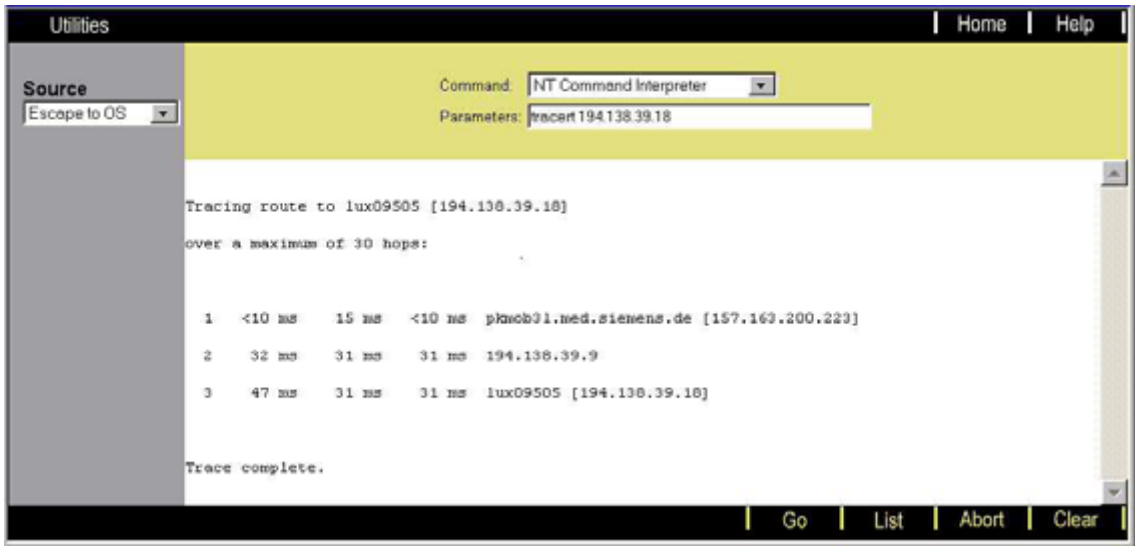

Fig. 7: tracert ok

The tracert 194.138.39.18 command performs a connection test to the SRS server in the Fürth extranet. All gateways used between the syngo system and the SRS router are listed. In our example, gateway 157.163.200.223 is used to connect the SP syngo system to the SRS router in Fürth.

What to do if the tracert command times out:

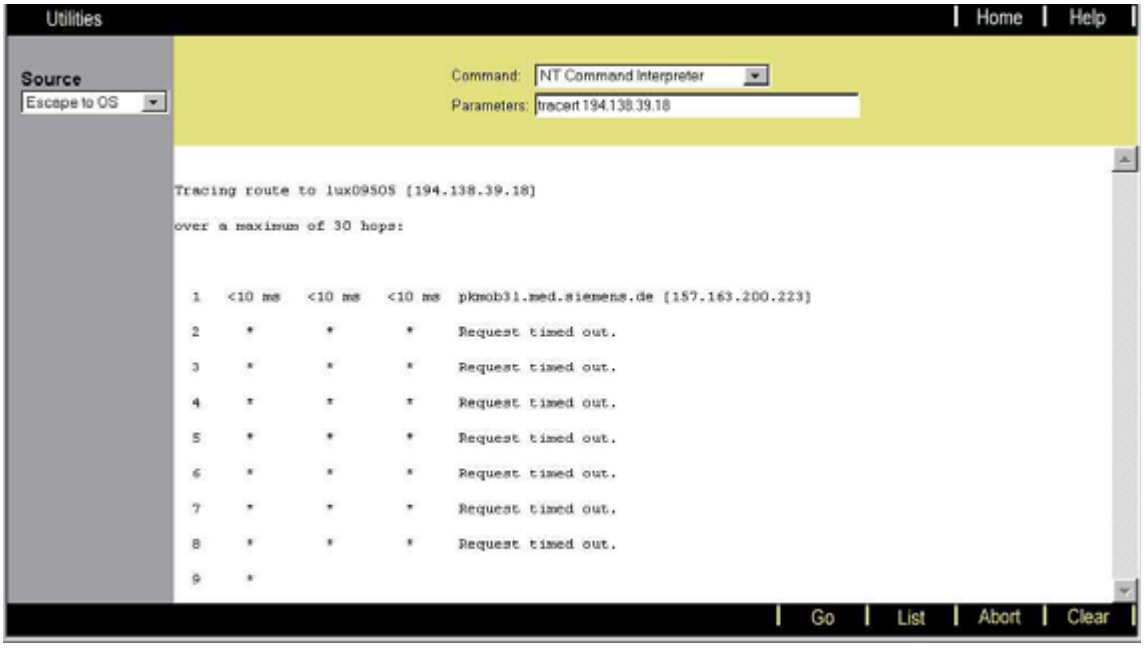

Fig. 8: tracert not ok

If the extranet of your time zone cannot be reached after several attempts, refer to:

- Check the network ports with the Pre-connect Tool, see documentation in (Troubleshooting / p. 60).
- Contact the network administrator of the hospital.
- Contact headquarters.
- Contact the (SRS Help Desk / p. 61).

Running the SRS Pre-connect Tool

The PM checks the connection between the system and the SRS servers with the Pre-connect Tool.

For information on downloading the latest Pre-connect Tool, refer to section SRS Pre-connect Tool in Additional Information.

Responsible person	Actions	Comment
Project Manager	Performance	The PM is responsible for the connection between the modality and SRS servers (Pre-connect Tool).
CSE	Performance	The CSE can also use the Pre-connect Tool, if necessary. (e.g. for troubleshooting during the subsequent configuration process).

Enable remote access based on syngo

The Siemens remote access mode setting is not covered by the Backup & Restore function. After SW installation, the Siemens remote access mode must be selected.

For syngo-based systems, select Options/Service/Remote service.

NOTE

Depending on your syngo version and on the system language, the service options may differ slightly.

- **Options/Remote service**
- **Options/Service/Remote service**
- **Options/Remote service**
- **Options/Service/Remote service**

- Enable remote access

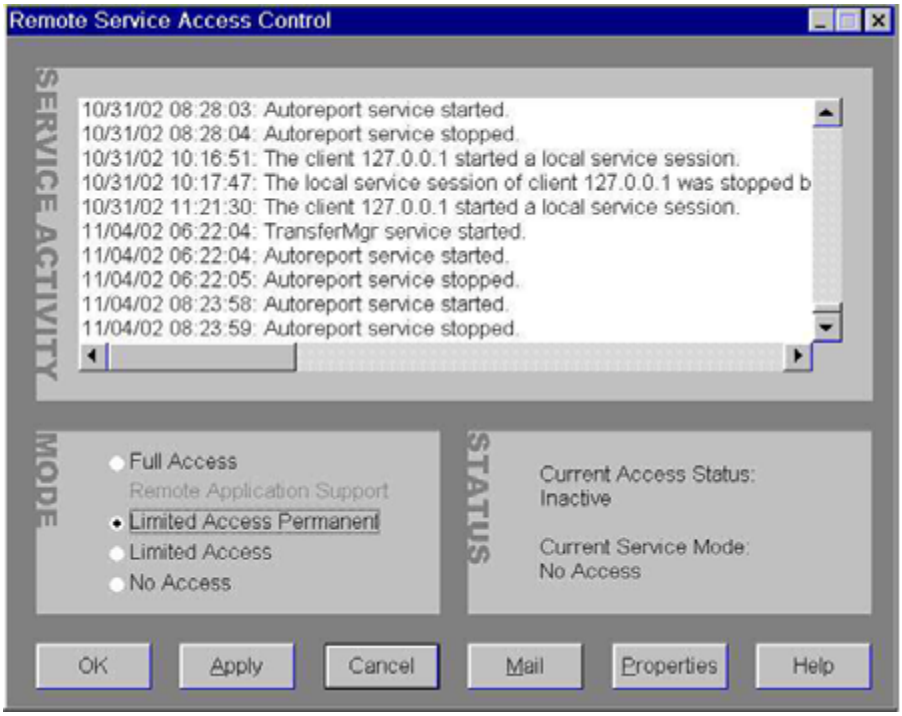

Fig. 9: Remote access mode

After consulting with the customer, enable the agreed-upon mode, e.g., Limited Access Permanent.

Access level	Comment
Full Access	The customer cannot continue to work; includes additional rights for several test tools available by remote access.
Limited Access Permanent	The customer can continue to work; limited rights for test tools; permanent remote access possible
Limited Access	The customer can continue to work; limited rights for test tools; remote access possible for a certain time as configured under Properties (default, e.g. 2 hours)
No Access	No remote access possible

Enter the country code and the customer ID

In some cases remote service uses data for the country code and customer ID.

Under Local service/Configuration/Site info, enter the following data:

- Country code for eg. "DE=Germany"
  For the list of country codes, see Additional Information.
- Customer ID, 7 digits of the local customer ID

Configure FTP transfer based on syngo

Configuration of the SRS target (host) used for FTP service

1. Go to local service
2. Select “Configuration”
3. On the configuration navigation page, select “FTP”

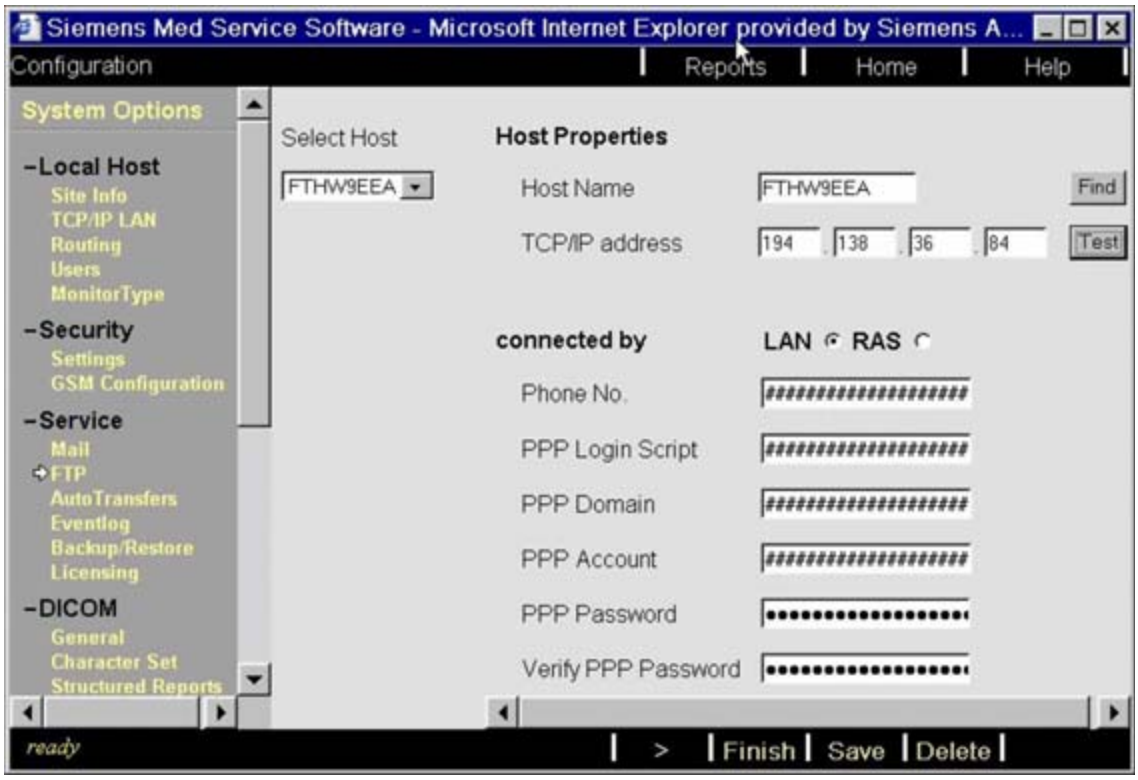

Fig. 10: FTP configuration

4. For your time zone, see (SRS access server / p. 9), define the new host name and enter the appropriate IP address.
5. Select “connected by LAN”.
6. Click “Save”

Definition of the FTP target

1. In “Service” select configuration “FTP”.
2. Check the SRS target (Configuration of the SRS target (host) used for FTP service / p. 35).

   Push the “test” button twice in succession to check the connection to the SRS server.

3. Click “>” to proceed to page two of Configuration/FTP

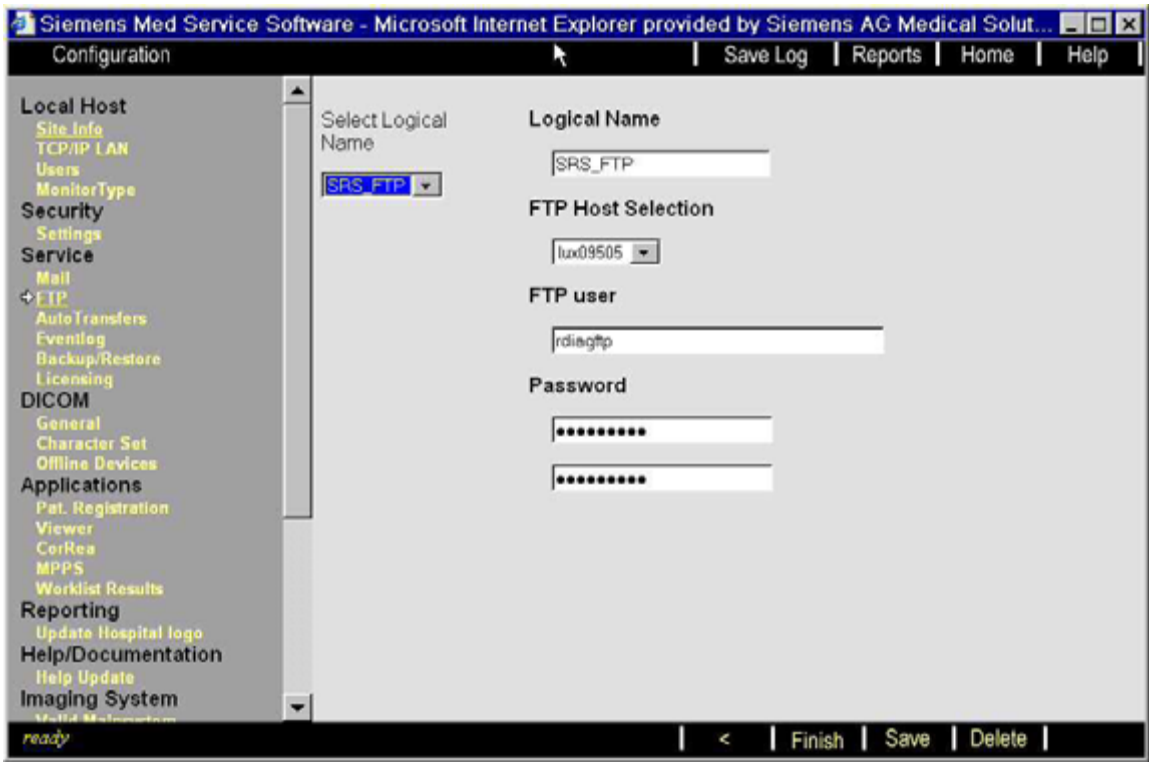

Fig. 11: FTP account

4. Define a new logical name: --> “SRS_FTP”
5. For "FTP host selection," select the host target as previously configured, see (SRS access server / p. 9).
6. In the “FTP user” field, enter: rdiagftp
7. In the “Password “ field, enter the password from the password list in the Intranet: see (Passwords / p. 62).
8. Confirm the password in the second line!
9. Click “Save”

Create a test file to check FTP transfer

To check the FTP service, create a file for transfer:

1. Log in to local service or remote service.
2. Click “Event Log”.
3. Select “Severity”: All
4. Select “Facility”: Service
5. Accept the current time range (date).

6. In the “Extract” field, enter a file name for the event log file, e.g.:

   “ut1005_27_10_2003_EventLog.txt”

   (ut = rdiag prefix of product

   1005 = system serial number

   27_10_2003 = date created)

7. Select “Go”.

   The file ut1005_27_10_2003_EventLog.txt will be written to C:\<%MEDHOME%>\service\extract.

   %MEDHOME% is a system variable depending upon the product ; to see the variable, type “set MEDHOME” in a cmd - box.

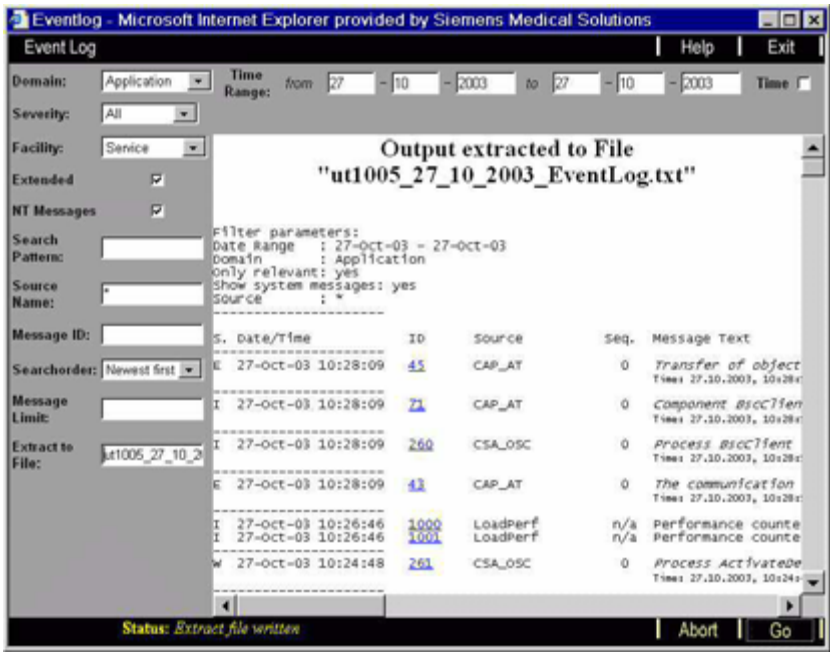

Fig. 12: Event Log data written to...

Check FTP transfer

1. Select “File & image tools” from the service software home menu.
2. Select “Source”: File
3. Select “Action”: Transfer from system
4. Select “File type”: Any file
5. Select “Site directory”: “C:\<%MEDHOME%>\service\extract”.

   %MEDHOME% is a system variable depending upon the product ; to see the variable, type “set MEDHOME” in a cmd - box.

6. Select the file to be transferred to the Siemens remote server, in this case ut1005_27_10_2003_EventLog.txt.

7. Press “Go” to start the file transfer via FTP:

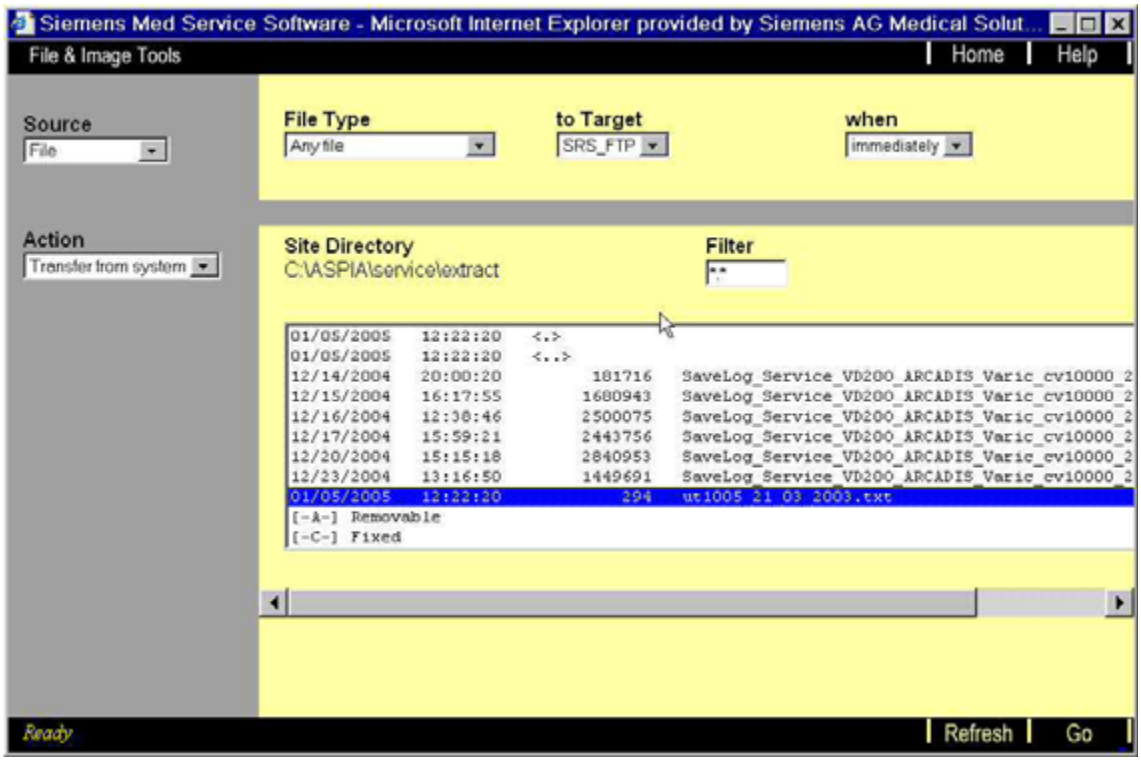

Fig. 13: File and image tool

The transfer manager queue opens and displays the status of the transfer.

Double-check the service activity windows under FTP check. No error should have occurred (wait approx. 5 minutes to check the output). In case of errors, refer to the “Troubleshooting” section for detailed information.

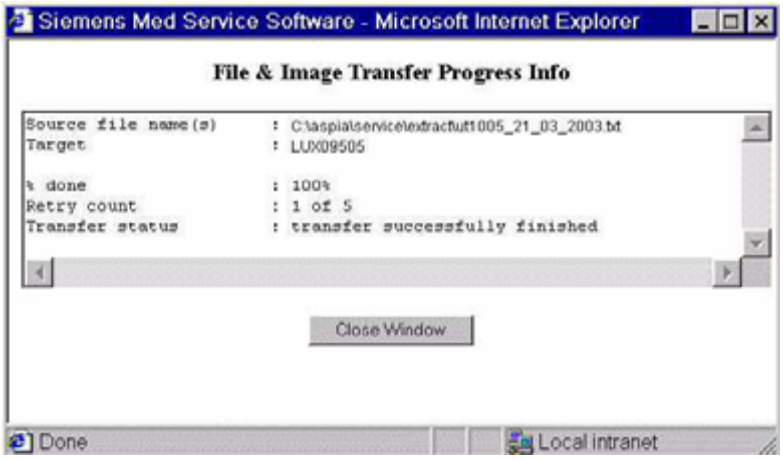
Siemens Med Service Software - Microsoft Internet Explorer
File & Image Transfer Progress Info
Source file name(s) : C:\aspia\service\extract\ut1005_21_03_2003.txt
Target : LUX09505
% done : 100%
Retry count : 1 of 5
Transfer status : transfer successfully finished
Close Window
Done
Local intranet

Fig. 14: FTP transfer

Configure access to the knowledge base based on syngo

Configure the access to Knowledge base

The CS knowledge base is accessible from the systems connected via a router (ISDN or DSL) or via VPN to the SRS server.

The SRS access server has to be configured as the proxy server in Internet Explorer.

Internet Explorer settings

The SRS access server functions as a proxy server between the syngo system and the intranet. Configure the IE browser as follows:

- Open local service by selecting Options/Local service or Options/Service/Local service.
- The service login platform is displayed and has to be activated; this is shown by the blue line at the top of the frame.

Fig. 15: Local Service

- Enter Ctrl + N on the keyboard to open a new browser window via the taskbar or open the browser by entering "iexplorer" in the command line (Utilities/Escape to OS).

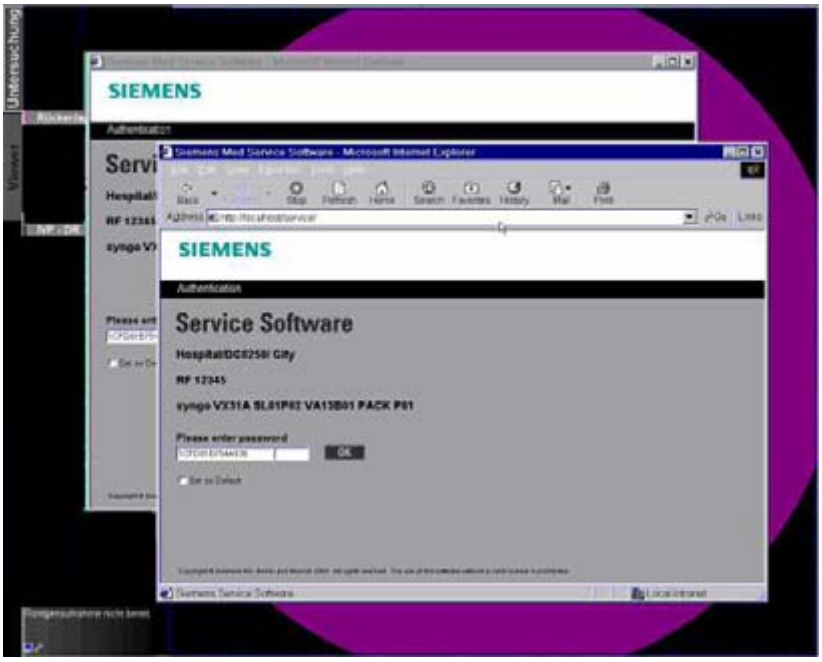

Fig. 16: New browser

- On the taskbar, select Tools --> Internet options --> Connections --> LAN settings.

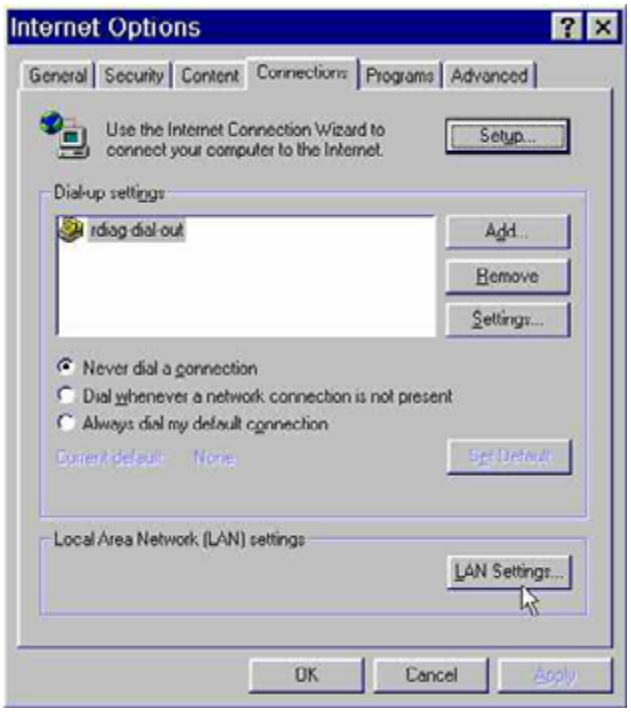

Fig. 17: Browser option

- Within the screen (LAN settings figure), enable "Use a proxy server" and ensure that "Bypass proxy server for local address" is selected.

- Click the "Advanced" button.

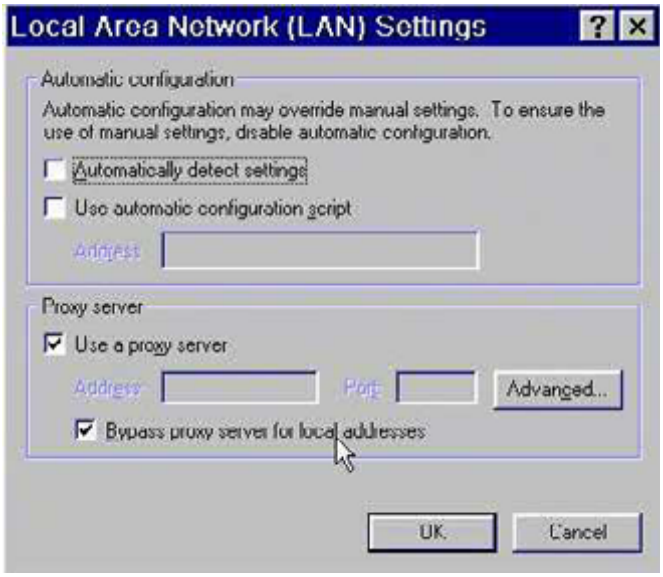

Fig. 18: LAN setting

- Enter the configured SRS server as the proxy address (see table below).

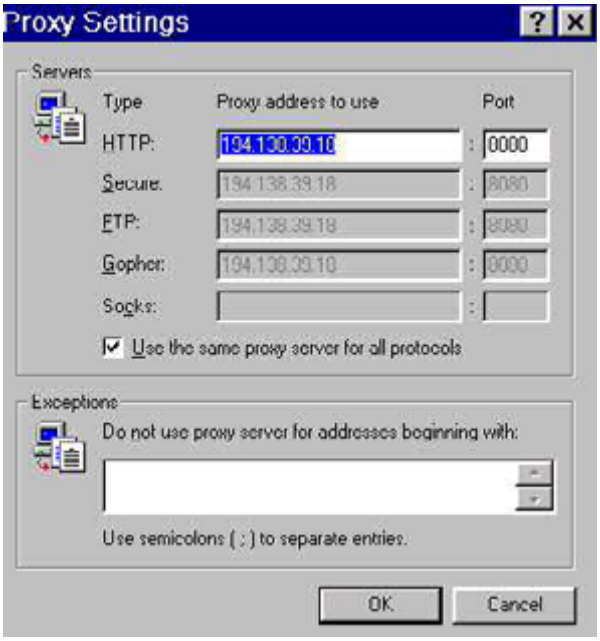

Fig. 19: Proxy ports

Tab. 1 SRS server IP addresses and host names

SRS-Server Location	IP-address (without Outside NAT)	If Outside NAT used, type the corresponding IP address in the field
Europe (Germany)	**194.138.39.18**	Replace the left IP address with the IP address given by the hospital network administrator.
America (USA)	**129.73.116.92**	Replace the left IP address with the IP address given by the hospital network administrator.
Asia (Singapore)	**194.138.243.178**	Replace the left IP address with the IP address given by the hospital network administrator.
Port number	**8080**	

- Enable "Use the same proxy server for all protocols" and save the entry with "OK".
- Bypass the subsequent pages with "OK" to access the CS knowledge base.
- Set the remote access mode to "limited access" or "limited access permanent".
- Open local service by selecting Options/Local service or Options/Service/Local service.
- The service login platform is displayed. Enter Ctrl + N on the keyboard to open a new browser window with the taskbar.
- Enter the address https://www-tdkb.med.siemens.de
- Reply to the security alert message window with "OK".

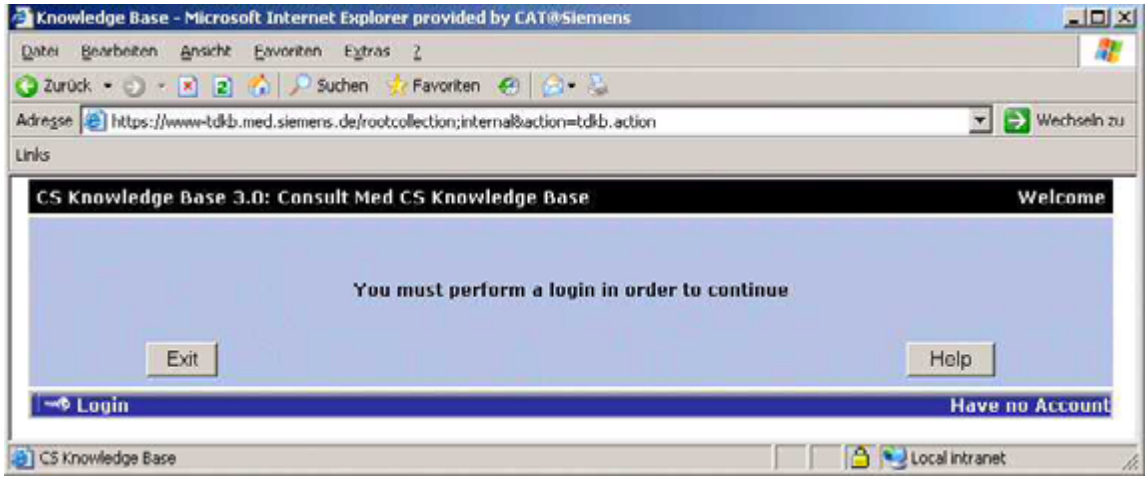

Fig. 20: CS Knowledge Base login

- Log in with your CS knowledge base user name and password.

NOTE

If you cannot access the CS knowledge base:

Click "Have no account". Find the "Administrator Med Meta Directory" for your country in the table below. Notify your administrator. He/she will make the necessary entries. You will receive your user name and password via e-mail.

General prerequisites

NOTE	**System Management is not released for VB13C.**

System Management (SM) must be deactivated and then activated in the following cases:

NOTE	**SM deactivated / activated when Inside NAT or Outside NAT is used and the IP addresses are changed.**

NOTE	**SM deactivated / activated when the system name has changed.**

NOTE	**SM deactivated / activated when the product software has been updated with a major version number change,** **e.g. update from VB10 to VB20.**

NOTE	**SM deactivated / activated when the values for material number or serial number have been changed (in case of incorrect values).**

Before setting up the System Management functionalities, check the following prerequisites:

- The SRS router/VPN configuration and the server configuration must be performed.
- Check whether the MNP source files are installed on the system.

  The MNP source files are preinstalled in the path: %MEDHOME%\service\mwtools
- The information regarding usage of Inside NAT or Outside NAT must be available and provided by the project manager.
- Perform a simple check of the connectivity to the SRS environment
  a) From the service software home menu, select Utilities -> Escape to OS
  b) Under Command, select NT Command Interpreter
  c) Within the NT Command Interpreter under parameters, enter one of the following commands and execute it by pressing <CR> or clicking <GO>.

  The tracert program takes a while before the data are displayed.

  When the mouse is moved into the frame, the hourglass indicates that the program is running.

  tracert <ip address from MNP access server see: (System management servers / p. 9) >

NOTE	**It may take some time to establish the connection.** **As a result, the tracert program may time out.** **Repeat the tracert command and check the function again.** **Do not continue with the installation if the connectivity test fails.**

NOTE	**Tracert and ping may not permitted by the hospital, but the rest of the functionality may work as wanted.** **e.g. for permitted: country UK, VPN over COA (customer router).**

- Advanced check of the connectivity to the SRS environment
  Run the Pre-connect Tool, see: (SRS Pre-connect Tool / p. 62).
  For a description, see: (Troubleshooting / p. 60).

Activating system management

The following chapters describe the procedure for activating System Management.

1. Activate the option “System Management”

1. Select Local Service --> Configuration
2. In the window click “System Options”

Fig. 21: Page -> Service -> Configuration -> System Options

3. Click “Next”

4. In the next window enable the “System Management” checkbox.

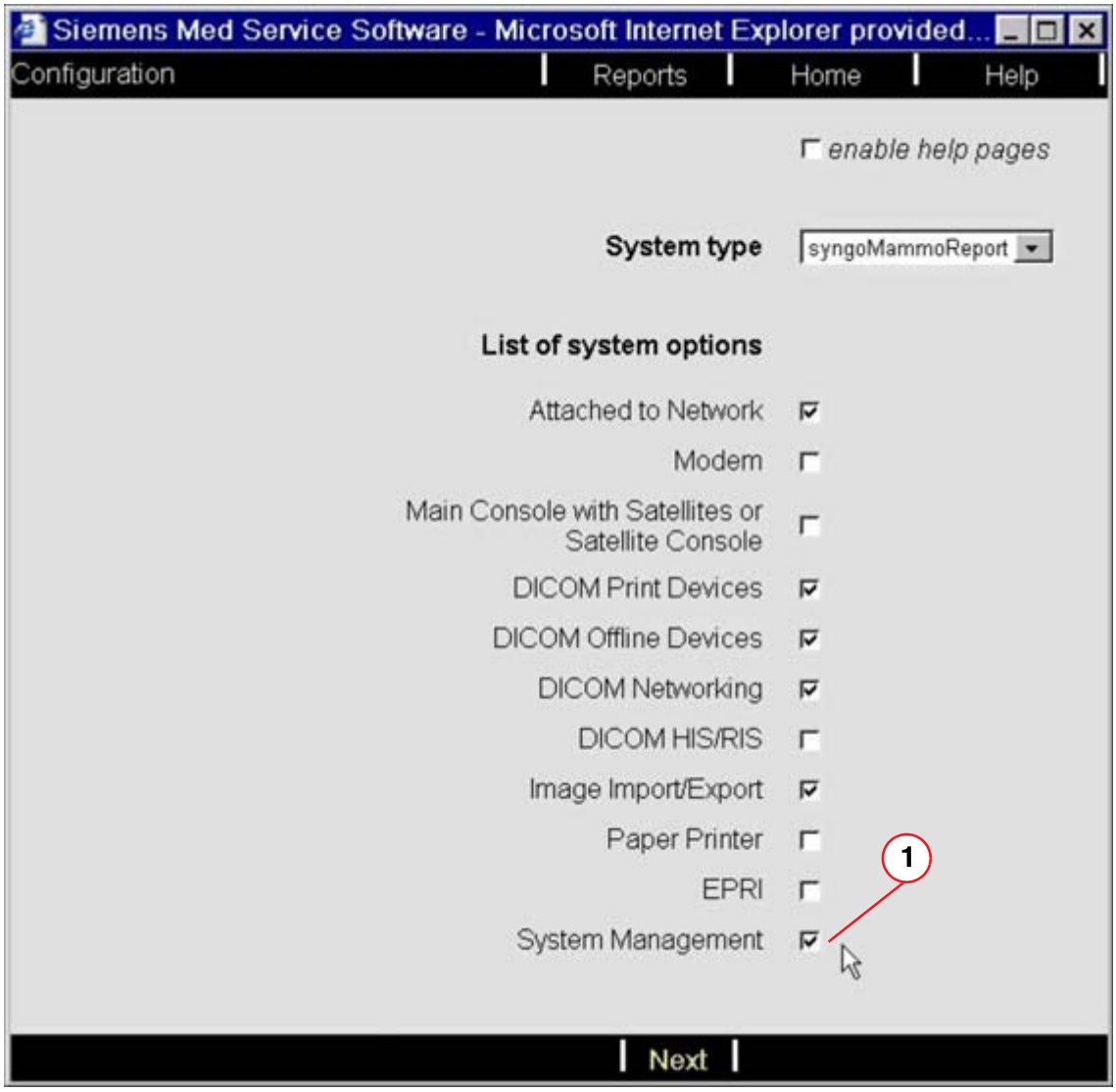

Fig. 22: Activate System Management
Pos. 1 “System Management” checkbox

5. Click “Next” twice.

2.1. Configuration of SM without NAT

NOTE	**Default settings mean:** **Configuration without Inside or without Outside NAT**

The following steps describe the configuration without NAT options.

1. Open the “Routing” page

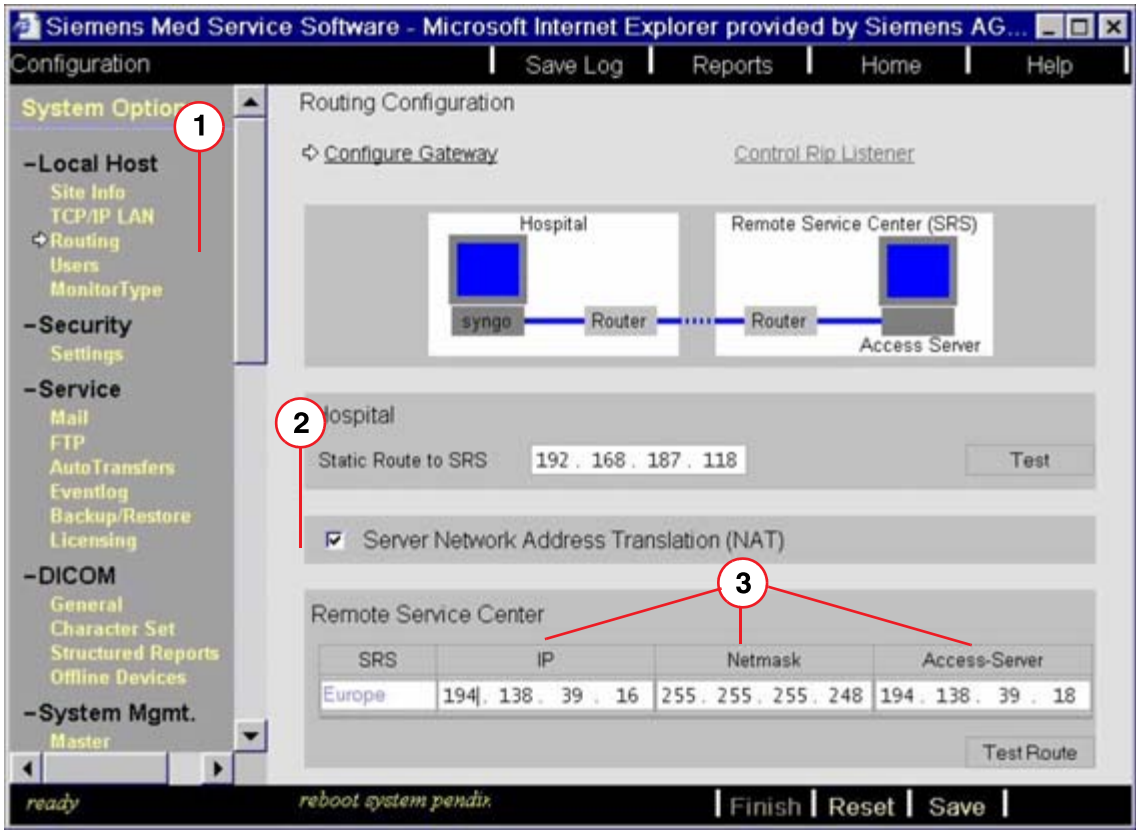

Fig. 23: Routing page with Outside NAT option activated

2. Checkbox **pos. 2** must be **deactivated**.

   Pos. 3 is automatically configured for the corresponding time zone.

3. Click “Save”

4. Open the following page: “System Mgmt. --> Master”

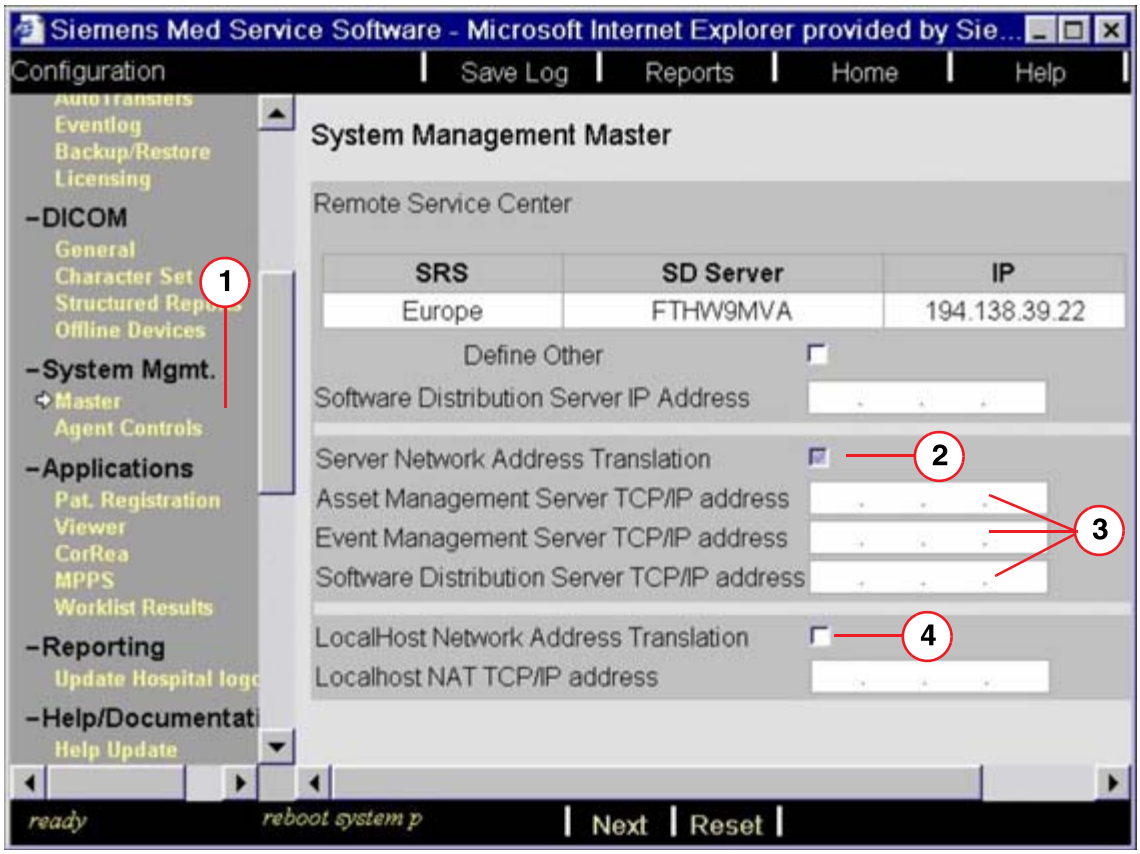

Fig. 24: SRS master page with Outside NAT option activated

5. The values for the “Remote Service Center” (e.g. Europe) will be automatically configured. The option “Define Other” will be only used for test cases.
6. Checkbox **pos. 2** is **deselected**, and checkbox **pos. 4** must be **deselected**.

2.2. Configuration of SM with Inside NAT

NOTE	**Inside NAT also can be called:** **L-NAT, localhost NAT, source NAT, client NAT**

Inside NAT description:

- Among other things, Inside NAT makes it possible to map a private IP address to a public IP address.
- In addition, Inside NAT is used when a customer is already using a private IP address and this cannot be changed easily to a public IP address.
- In most cases, Inside NAT is implemented in the SRS router. The system IP address remains unchanged in the client network; when the system data is sent via the SRS router, the IP address is translated.

How to find out about Inside NAT

- Compare the system IP address (DICOM connection) to the IP address on the SRS server. Contact the SRS Help Desk to obtain the IP address of the SRS server.

Local IP address [1]				IP address on SRS server [2]			

1. DICOM connection
2. system IP address on the SRS server

➪ If both IP addresses are the same, Inside NAT is not used;
if the IP addresses are different, Inside NAT is used.
The Inside NAT IP address is the IP address that is entered on the SRS server.

NOTE **If you are not sure, ask the SRS help desk.**

The following steps describe the configuration of the option “Inside NAT”.

1. Open the following page: “System Mgmt. --> Master”

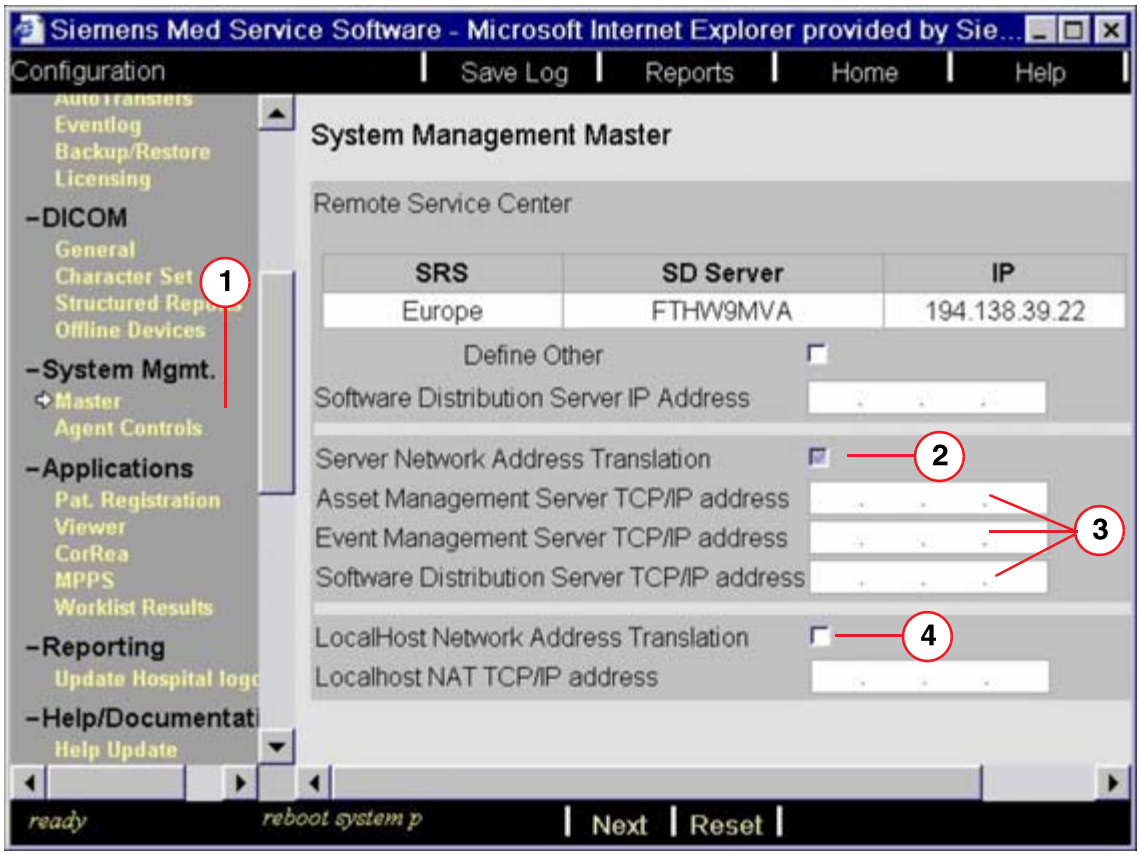

Fig. 25: SRS master page with Outside NAT option activated

2. The time zone (e.g. Europe) will be automatically set.
3. Activate checkbox “Localhost Network Address Translation”, see pos. 4
4. Enter the Inside NAT IP address given by the hospital network administrator in the field “Localhost NAT TCP/IP address”

5. Click “Next”

2.3. Configuration of SM with Outside NAT

NOTE

Outside NAT also can be called:

- S-NAT (can be confused with source NAT, which is directly the opposite)

- server NAT, destination NAT, even manager NAT

Outside NAT description

In some customer networks, it is possible that communication is permitted only within a particular IP address range.

Because of this, it can happen that communication from the FL-C to the System Management servers is not possible.

To clarify whether Outside NAT is being used, contact the customer's network administrator or the SRS help desk.

In addition, when using Outside NAT, the router must be configured accordingly. This must be performed prior to configuration in the FL-C.

NOTE

If you are not sure, ask the SRS help desk.

The following steps describe the configuration of the option “Outside NAT”.

1. Open the following page “Routing”.

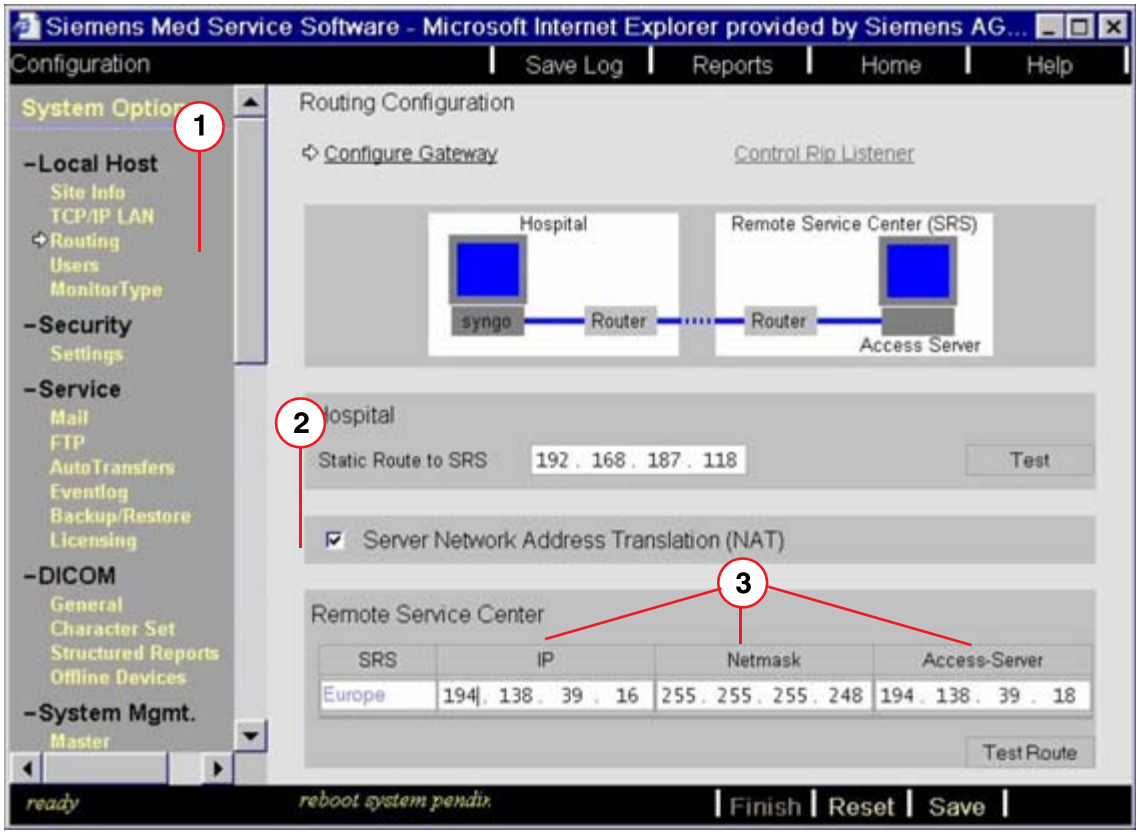

Fig. 26: Routing page with Outside NAT option activated

2. Checkbox “Server Network Address Translation (NAT)” **pos. 2** must be **activated**.
3. In **pos. 3**, enter the values for: IP Address, Netmask, and Access Server given by the hospital network administrator.
4. Click “Save”.

5. Open the following page: “System Mgmt. --> Master”

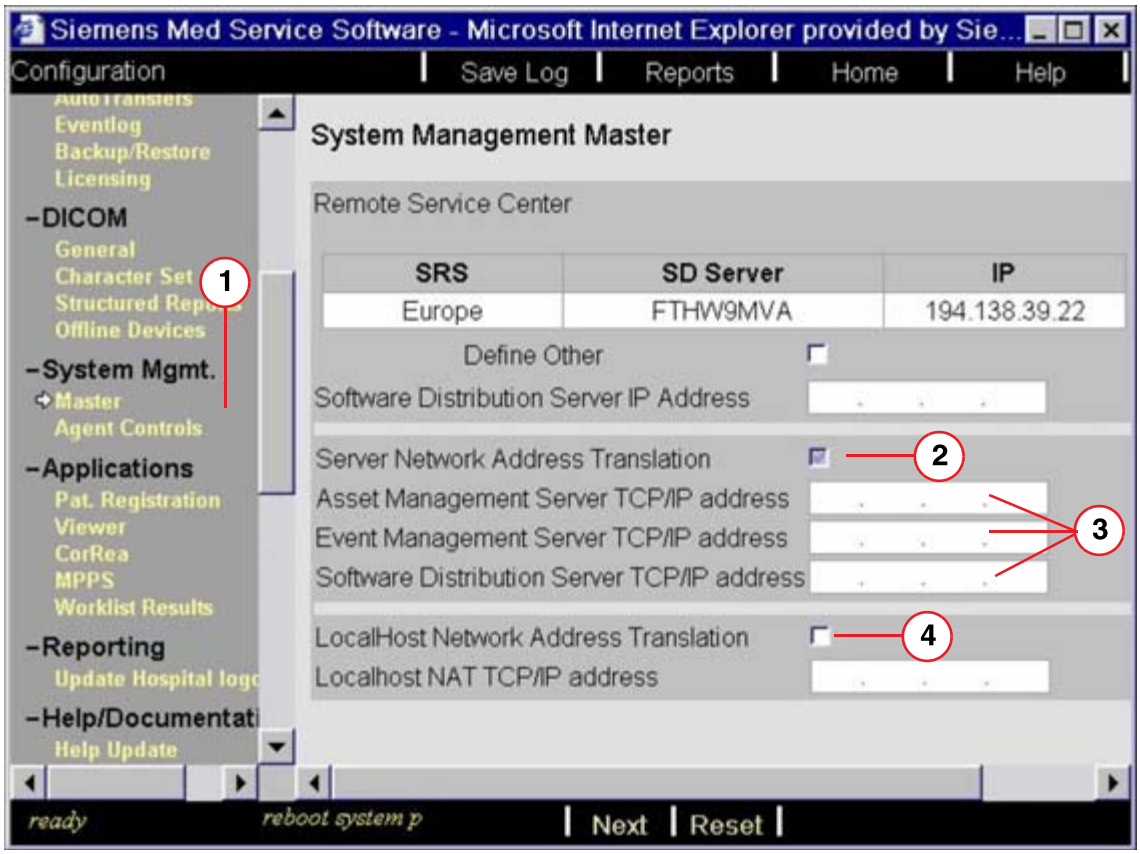

Fig. 27: SRS master page with Outside NAT option activated

6. The time zone (e.g. Europe) will be automatically set.
7. Pos. 2 now shows the automatically activated option “Server Network Address Translation”.
8. Depending on the time zone in which the system is located, the IP addresses in **pos. 3** for the:

   Asset Management Server (e.g. Europe 194.138.39.21)

   Event Management Server (e.g. Europe 194.138.39.20)

   Software Distribution Server (e.g. Europe 194.138.39.22)

   must be **replaced** by the IP address given by the hospital network administrator.

NOTE	**For any questions ask the SRS help desk.**

9. Checkbox **pos. 4** must be **deselected** (option Inside NAT, will not be used in this scenario).
10. Click “Next”

3 . Start of activation procedure

1. Open the following page “System Mgmt. --> Agent Controls”

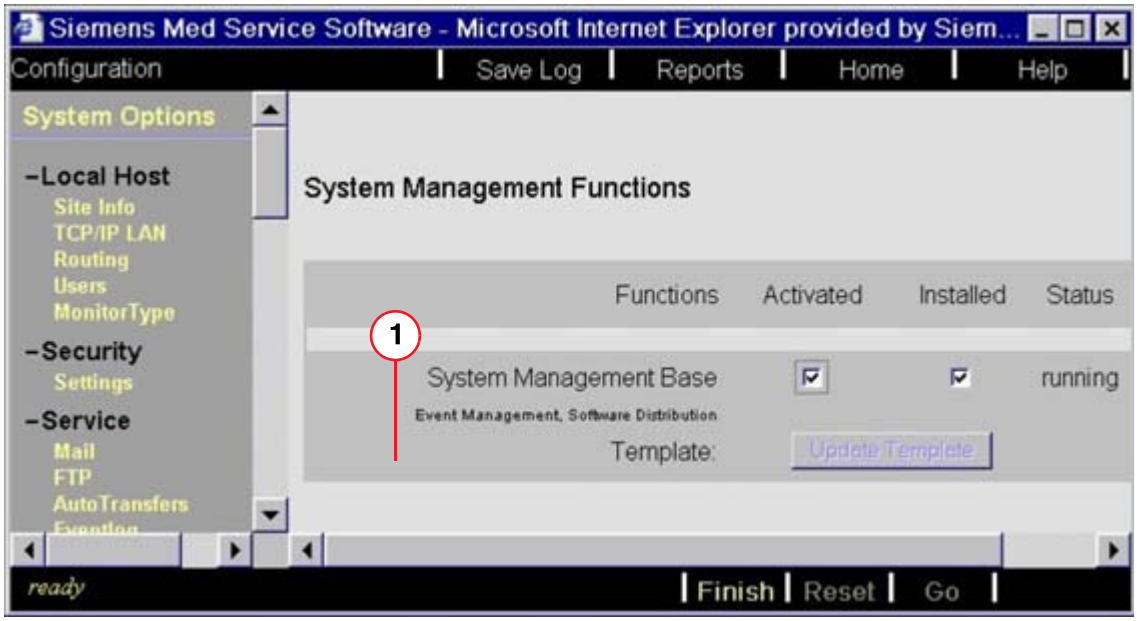

Fig. 28: MNP status "running", with template download in progress

2. Activate the **two** checkboxes as shown, click **“GO”**, and wait for status **“running”**

   The system management processes “registration” and “installation of template” will start in the background (the template, see pos.1, will be not displayed.)

NOTE	**This takes approximately < 15 minutes! Please be patient.** **Do not reboot the system.**

3. Wait until the template version in the next figure, pos. 2, is displayed.

   To refresh this page, click the “Finish” and “Agent Controls” buttons (pos. 1) in sequence in two minute increments.

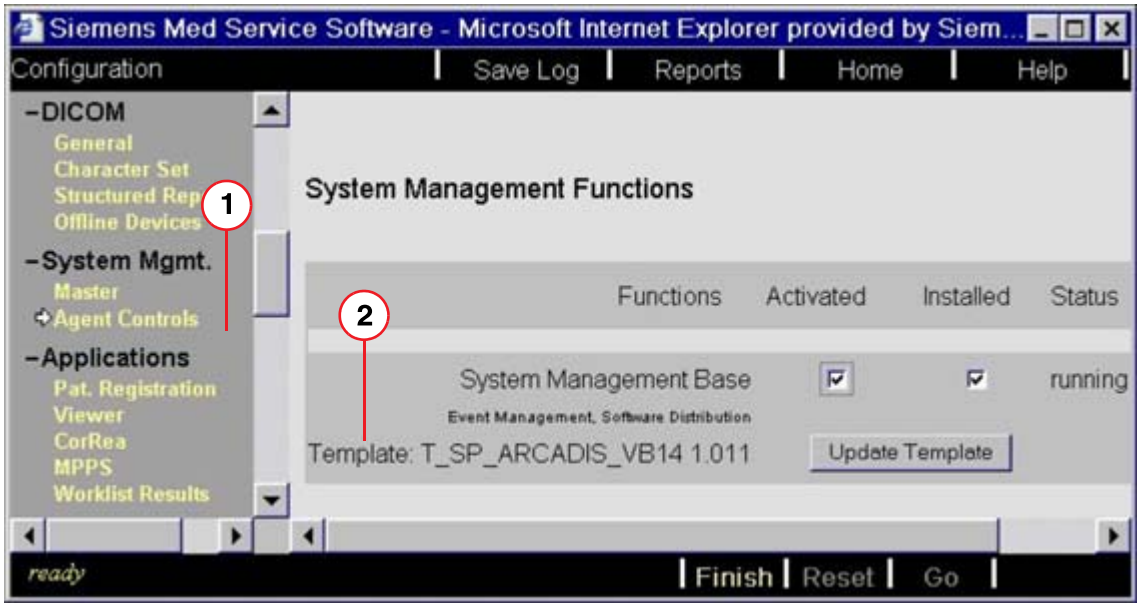

Fig. 29: MNP status "running", with template

4. Click “**Finish**”
5. If the installation of System Management fails, see Troubleshooting or call the SRS help desk.

4. Check the functionality of all MNP components

1. Check whether the template is installed
   a) Open a command box with administrative rights
   b) Go to the directory C:\syngo\service\mwtools
   c) Type sysmgmt_install.exe - s

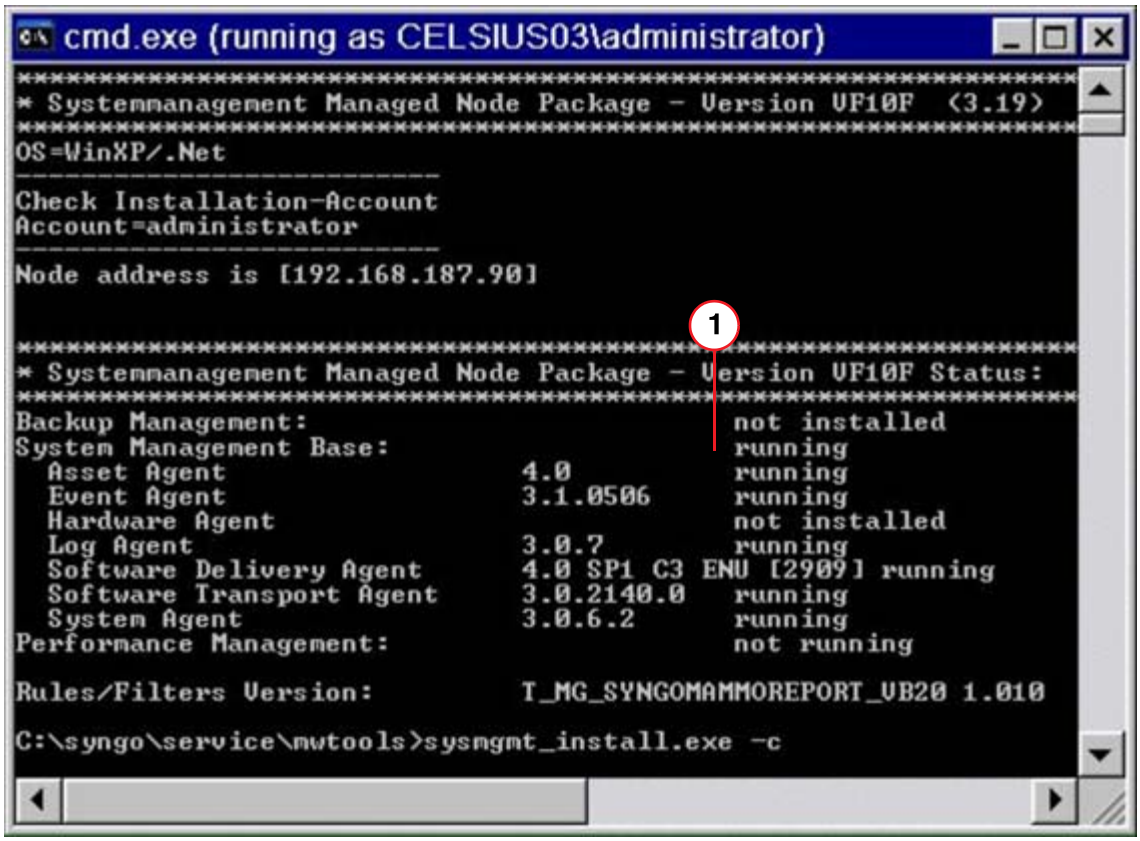
cmd.exe (running as CELSIUS03\administrator)
* Systemmanagement Managed Node Package - Version VF10F (3.19)
OS=WinXP/.Net
Check Installation-Account
Account=administrator
Node address is [192.168.187.90]
1
* Systemmanagement Managed Node Package - Version VF10F Status:
Backup Management: not installed
System Management Base: running
Asset Agent 4.0 running
Event Agent 3.1.0506 running
Hardware Agent not installed
Log Agent 3.0.7 running
Software Delivery Agent 4.0 SP1 C3 ENU [2909] running
Software Transport Agent 3.0.2140.0 running
System Agent 3.0.6.2 running
Performance Management: not running
Rules/Filters Version: T_MG_SYNGOMAMMOREPORT_VB20 1.010
C:\syngo\service\mwtools>sysmgmt_install.exe -c

Fig. 30: MNP status running complete with template
Pos. 1 see Status running

The following results must be displayed:

- The System Management Base will display the status “running”
- The template “T_SP_Arcadis_VB14 1.0xx” will be displayed (xx >= 10).

If one of these results is not displayed, wait **<= 10 minutes** and type sysmgmt_install.exe - s again.

For help, see (Troubleshooting / p. 60) or (SRS Help Desk / p. 61).

Deactivating System Management

Procedure for deactivating System Management

1. Select Local Service --> Configuration
2. **Deactivate** the two checkboxes, click **"GO"** and wait for status **"not running"**

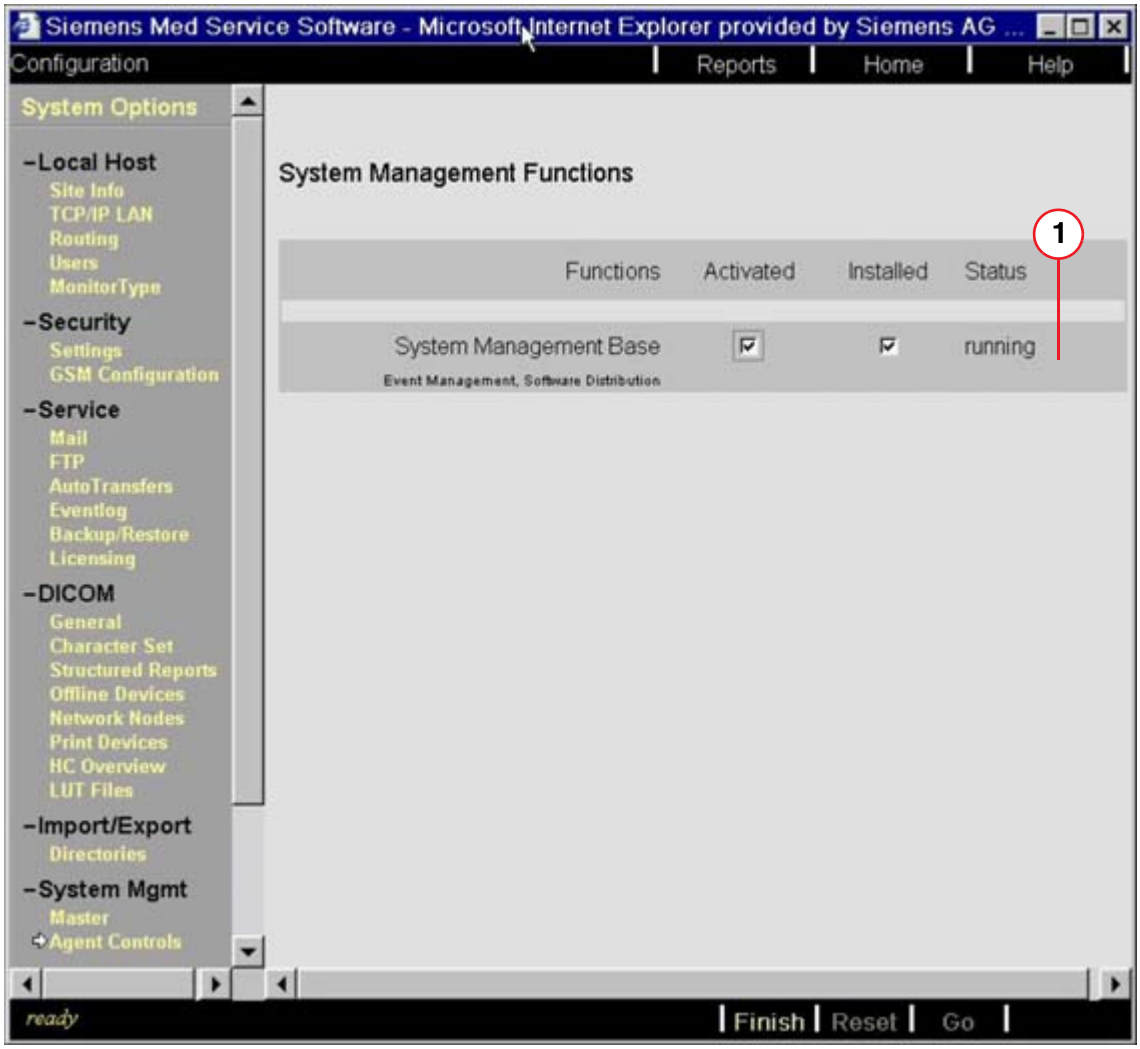

Fig. 31: MNP status running complete

Pos. 1 see Status running

The System Management processes "deregistration from SRS server" and "deinstallation of all MNP components" will be started in the background.

NOTE	**Do not reboot the system.**

NOTE	**This takes approximately < 10 minutes! Please be patient.**

3. In the next window, click “System Options”

Fig. 32: Page -> Service -> Configuration -> System Options

Type “Next”

4. In the next window **deactivate** the checkbox “System Management”.

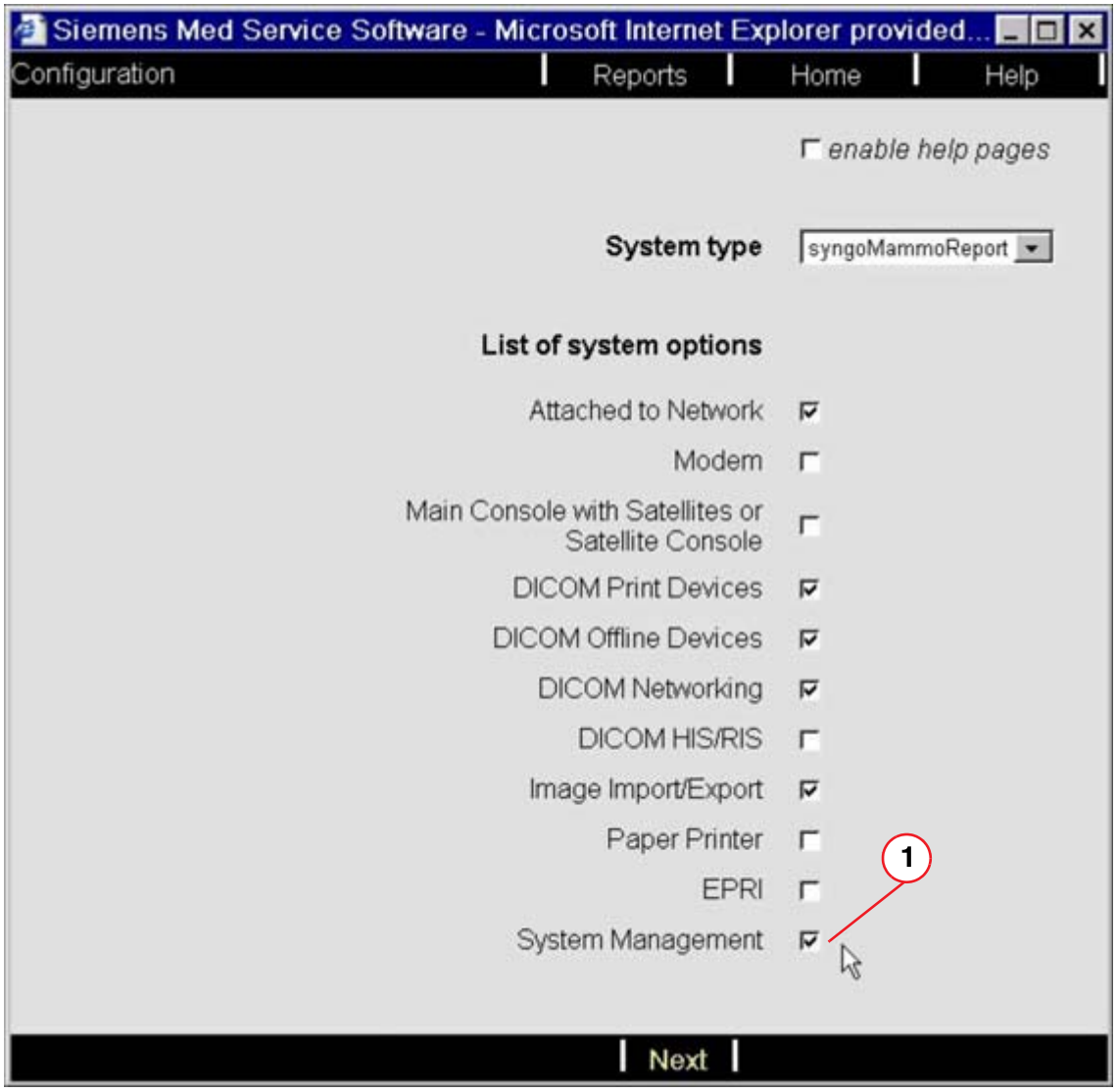

Fig. 33: Activate System Management
Pos. 1 “System Management” checkbox

Click **“Next”** twice.

5. If the deinstallation of System Management fails, see (Troubleshooting / p. 60) or see (SRS Help Desk / p. 61).

The SRS troubleshooting is available under:

Siemens Intranet --> CS --> For Service --> SP Systems --> Surgery -->
CBDOC --> Service --> Siemens Remote Service --> SRS Troubleshooting Guide

Additional information

SRS portal access

A personal account is required on the SRS portal to access data and to connect to systems.

For accounts, see “MMD Country Admin”:

http://cs.med.siemens.de/cms/en/tools/mmdcountryadmin/default.asp

SRS Help Desk

In case of questions or any problems please contact one of the following Help Desks:

- SRS Help Desk worldwide

  Phone: +49 919118 8080 Code 191

  Fax: +49 9131 84 13 7388

  E-Mail: RemoteServer.med@siemens.com

  Service days: Monday - Friday

  Service time: 7:00 AM - 10:00 PM (UTC+1)

- SRS Help Desk (USA only)

  Phone: +1 919 319-2756

  E-Mail: csg.srs.med@siemens.com

  Service days: Monday - Friday

  Service time: 8:30 AM - 7:00 PM EST

SRS Checklist

The **SRS Checklist** is available in the **Siemens Intranet**; see **CS homepage**:

For Service > Product Information > Siemens Remote Service > CB-DOC >

> Installation > System > Installation Instructions > SRS Final Configuration Checklist

The checklist can be sent directly to: Srs_final.med@siemens.com

The **SRS router order form** is available in the **Siemens Intranet**; see **CS homepage**:

For Service > Product Information > Siemens Remote Service > CB-DOC >

> Planning > System > Planning Guide > Router order form

SRS Toolkit

The SRS Toolkit is available under:

Siemens Intranet see **CS homepage**:

> For Service > Product Information > Siemens Remote Service > CB-DOC

SRS Pre-connect Tool

The SRS Pre-connect Tool is available in **Siemens Intranet** see **CS homepage**:

For Service > Product Information > Siemens Remote Service > CB-DOC >

> Installation > System > Installation Instructions > Pre-connect Tool

Passwords

The only password needed during the SRS configuration is the connection password for access via FTP to the SRS access server (account “rdiagftp”).

The password is listed in the CS Knowledge Base:

http://www-tdkb.med.siemens.de/rootcollection;internal&action=tdkb.action

Using the **Search in KB** button with the **Type of Information** checkbox set to **[P]Password List**, you will get the latest passwords for your BU.

Country codes

Tab. 2 ISO 3166 country codes

Afghanistan	AF	Grenada	GD	Russian Federation	RU
Albania	AL	Guadeloupe	GP	Rwanda	RW
Algeria	DZ	Guam	GU	S. Georgia and S. Sandwich Islands	GS
American Samoa	AS	Guatemala	GT	Saint Kitts and Nevis	KN
Andorra	AD	Guinea	GN	Saint Lucia	LC
Angola	AO	Guinea-Bissau	GW	Saint Vincent & the Grenadines	VC
Anguilla	AI	Guyana	GY	Samoa	WS
Antarctica	AQ	Haiti	HT	San Marino	SM

Antigua and Bermuda	AG	Heard and McDonald Islands	HM	Sao Tome and Principe	ST
Argentina	AR	Honduras	HN	Saudi Arabia	SA
Armenia	AM	Hong Kong	HC	Senegal	SN
Aruba	AW	Hungary	HU	Seychelles	SC
Australia	AU	Iceland	BS	Sierra Leone	SL
Austria	AT	India	IN	Singapore	SG
Azerbaijan	AZ	Indonesia	ID	Slovenia	SI
Bahamas	BS	Iran	IR	Slovak Republic	SK
Bahrain	BH	Iraq	IQ	Solomon Islands	SB
Barbados	BB	Ireland	IE	Somalia	SO
Bangladesh	BD	Israel	IL	South Africa	ZA
Belarus	BY	Italy	IT	Spain	ES
Belgium	BE	Jamaica	JM	Sri Lanka	LK
Belize	BZ	Japan	JP	St. Helena	SH
Benin	BJ	Jordan	JO	St. Pierre and Miquelon	PM
Bermuda	BM	Kazakhstan	KZ	Sudan	SD
Bahamas	BS	Kenya	KE	Suriname	SR
Bhutan	BT	Kiribati	KI	Svalbard & Jan Mayen Islands	SJ
Botswana	BW	Korea (North)	KP	Swaziland	SZ
Bolivia	BO	Korea (South)	KR	Sweden	SE
Bosnia and Herzegovina	BA	Kuwait	KW	Switzerland	CH
Bouvet Island	I.I.	Kyrgyzstan	KG	Syria	SY
Brazil	BR	Laos	LA	Taiwan	TW
British Indian Ocean Territory	IO	Latvia	LV	Tajikistan	TJ
Brunei Darussalam	BN	Lebanon	LB	Tanzania	TZ
Bulgaria	BG	Liechtenstein	LI	Thailand	TH
Burkina Faso	BF	Liberia	LR	Togo	TG
Burundi	BI	Libya	LY	Tokelau	TK
Cambodia	KH	Lesotho	LS	Tonga	TO

Cameroon	CM	Lithuania	LT	Trinidad and Tobago	TT
Canada	CA	Luxembourg	LU	Tunisia	TN
Cape Verde	CV	Macau	MO	Turkey	TR
Cayman Islands	KY	Madagascar	MG	Turkmenistan	TM
Central African Republic	CF	Malawi	MW	Turks and Caicos Islands	TC
Chad	TD	Malaysia	MY	Tuvalu	TV
Chile	CL	Maldives	MV	Uganda	UG
China	CN	Mali	ML	Ukraine	UA
Christmas Island	CX	Malta	MT	United Arab Emirates	AE
Cocos (Keeling) Islands	CC	Marshall Islands	MH	United Kingdom	UK
Colombia	CO	Martinique	MQ	United States	US
Comoros	KM	Mauritania	MR	US Minor Outlying Islands	UM
Congo	CG	Mauritius	MU	Uruguay	UY
Congo, Democratic Republic	CD	Mayotte	YT	USSR (former)	SU
Cook Islands	CK	Mexico	MX	Uzbekistan	UZ
Costa Rica	CR	Micronesia	FM	Vanuatu	VU
Cote D'Ivoire (Ivory Coast)	CI	Monaco	MC	Vatican City State (Holy See)	VA
Croatia (Hrvatska)	HR	Moldova	MD	Venezuela	VE
Cuba	CU	Morocco	MA	Vietnam	VN
Cyprus	CY	Mongolia	MN	Virgin Islands (British)	VG
Czech Republic	CZ	Montserrat	MS	Virgin Islands (U.S.)	VI
Denmark	DK	Mozambique	MZ	Wallis and Futuna Islands	WF
Djibouti	DJ	Myanmar	MM	Western Sahara	EH
Dominica	DM	Namibia	NA	Yemen	YE
Dominican Republic	DO	Nauru	NR	Zambia	ZM
East Timor	TP	Nepal	NP	Zimbabwe	ZW

Ecuador	EC	Netherlands	NL
Egypt	EG	Netherlands Antilles	AN
El Salvador	SV	Neutral Zone	NT
Equatorial Guinea	GQ	New Caledonia	NC
Eritrea	ER	New Zealand (Aotearoa)	NZ
Estonia	EE	Nicaragua	NI
Estonia	EE	Niger	NE
Ethiopia	ET	Nigeria	NG
Falkland Islands (Malvinas)	FK	Niue	NU
Faeroe Islands	FO	Norfolk Island	NF
Fiji	FJ	Northern Mariana Islands	MP
Finland	FI	Norway	NO
France	FR	Oman	OM
France, Metropolitan	FX	Pakistan	PK
French Guiana	GF	Palau	PW
French Polynesia	PF	Panama	PA
French Southern Territories	TF	Papua New Guinea	PG
F.Y.R.O.M. (Macedonia)	MK	Paraguay	PY
Gabon	GA	Peru	PE
Gambia	GM	Philippines	PH
Georgia	GE	Pitcairn	PN
Germany	DE	Poland	PL
Ghana	GH	Portugal	PT
Gibraltar	GI	Puerto Rico	PR
Great Britain (UK)	GB	Qatar	QA
Greece	GR	Reunion	RE
Greenland	GL	Romania	RO

Initial version